aaa

aaa-certParams

The following operations can be performed on "aaa-certParams":

unset| show| set|

unset aaa certParams

Use this command to remove aaa certParams settings.Refer to the set aaa certParams command for meanings of the arguments.

Synopsis

unset aaa certParams

show aaa certParams

Displays the current client certificate configuration on the Citrix ADC.

Synopsis

show aaa certParams

Arguments

Output

twoFactor The state of the two-factor authentication.

userNameField The field in the certificate from which the username will be extracted.

groupNameField The field in the certificate from which the group will be extracted.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

set aaa certParams

Modifies the global configuration settings for certificate policies. The settings that you specify are used for all SSL-VPN virtual servers unless you use authentication policies to create a configuration for a specific SSL-VPN virtual server.

Synopsis

set aaa certParams

Arguments

userNameField Client certificate field that contains the username, in the format <field>:<subfield>.

groupNameField Client certificate field that specifies the group, in the format <field>:<subfield>.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

Example

To configure the default certificate parameters: set aaa certparams -userNameField "Subject:CN" -groupNameField "Subject:OU"

Related Commands

- set aaa parameter

Aaa

The entities on which you can perform NetScaler CLI operations:

aaa-global

The following operations can be performed on "aaa-global":

bind| unbind| show|

bind aaa global

Binds a policy globally.

Synopsis

bind aaa global [-policy <string>]

Arguments

policy Name of the policy to bind globally.

priority Priority to assign to the policy, as an integer. A lower number indicates a higher priority. Policies are evaluated in the order of their priority numbers. Minimum value: 0

windowsProfile Name of the negotiate profile to bind globally.

Example

bind aaa global -pol pol1

unbind aaa global

Unbind the policy from the global bind point.

Synopsis

unbind aaa global

Arguments

policy Name of the policy to be unbound.

windowsProfile Name of the negotiate profile to be bound.

show aaa global

Displays a list of policies that are currently bound to Global on the Citrix ADC.

Synopsis

show aaa global

Arguments

Output

policy Name of the policy to be unbound.

windowsProfile Name of the negotiate profile to be bound.

priority Priority of the bound policy

bindPolicyType Bound policy type

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

devno count stateflag

aaa-group

The following operations can be performed on "aaa-group":

bind| unbind| add| rm| show|

bind aaa group

Binds the specified AAA group to the specified resource. The resource can be a user, an Intranet IP address or range, a policy, or an Intranet application.

Synopsis

bind aaa group <groupName> (-userName <string> | (-policy <string>) | -intranetApplication <string> | -urlName <string> | (-intranetIP <ip_addr> <netmask>) | (-intranetIP6 <ip_addr|ipv6_addr|*> <numaddr>))

Arguments

groupName Name of the group that you are binding.

userName Bind a AAA group to the specified AAA user. If the specified user is bound to more than one group, the group expressions are evaluated, upon authorization, to determine the appropriate action.

policy Bind a policy to the specified AAA group.

priority Integer specifying the priority of the policy. A lower number indicates a higher priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value: 0 Maximum value: 2147483647

type Bindpoint to which the policy is bound.

Possible values: REQUEST, UDP_REQUEST, DNS_REQUEST, ICMP_REQUEST Default value: REQUEST

intranetApplication Bind the group to the specified intranet VPN application.

urlName Bind the group to the specified URL.

intranetIP Bind the group to the specified IP address or IP block. Normally you would bind the group to an IP address or range that your users use to access intranet resources.

netmask Subnet mask specifying an IP-address range to which to bind a AAA group.

gotoPriorityExpression Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

intranetIP6 Bind the group to the specified IP6 address or IP block. Normally you would bind the group to an IP6 address or range that your users use to access intranet resources.

numaddr Number of ipv6 address to be bound Minimum value: 1

Example

To bind an Intranet IP to the group engg: bind aaa group engg -intranetip 10.102.10.0 255.255.255.0

unbind aaa group

Unbinds the specified AAA group from the specified resource. The resource can be a user, an intranet IP address or range, a policy, or an intranet application.

Synopsis

unbind aaa group <groupName> (-userName <string> ... | (-policy <string>) | -urlName <string> | (-intranetIP <ip_addr> <netmask>) | (-intranetIP6 <ip_addr|ipv6_addr|*>))

Arguments

groupName Name of the group that you are unbinding.

userName Unbind the specified AAA group from the specified AAA user.

policy Unbind the specified policy from the specified AAA group.

type Bindpoint to which the policy is bound.

Possible values: REQUEST, UDP_REQUEST, DNS_REQUEST, ICMP_REQUEST Default value: REQUEST

intranetApplication Unbind the specified group from the specified intranet VPN application.

urlName Unbind the specified group from the specified URL.

intranetIP Unbind the specified group from the specified IP address or IP block.

netmask Subnet mask for the IP range in which the intranet application from which you are unbinding the policy resides. Required if the intranet application has multiple IP addresses bound to it. Not needed if the intranet application resides on a single IP address.

intranetIP6 IP6 address of the intranet application to which you are unbinding the policy.

numaddr Number of addresses for the IPv6 range in which the intranet application to which you are binding the policy resides. Required if the intranet application has multiple IPv6 addresses bound to it. Not needed if the intranet application resides on a single IP address. Minimum value: 1

Example

unbind aaa group engg -intranetip 10.102.10.0 255.255.255.0

add aaa group

Creates a AAA group and verifies the configuration to ensure that it is correct.

Synopsis

add aaa group <groupName>

Arguments

groupName Name for the group. Must begin with a letter, number, or the underscore character (_), and must consist only of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the group is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my aaa group" or 'my aaa group').

weight Weight of this group with respect to other configured aaa groups (lower the number higher the weight) Default value: 0 Minimum value: 0 Maximum value: 65535

Example

add aaa group group_ad

rm aaa group

Removes the specified AAA group.

Synopsis

rm aaa group <groupName>

Arguments

groupName Name of the group that you are removing.

show aaa group

Displays the current configuration of a AAA group.

Synopsis

show aaa group

Arguments

groupName Name of the group.

loggedIn Display only the group members who are currently logged in. If there are large number of sessions, this command may provide partial details.

Output

userName The user name.

policy The policy name.

priority Integer specifying the priority of the policy. A lower number indicates a higher priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000.

intranetApplication Bind the group to the specified intranet VPN application.

urlName The intranet url

actType intranetIP The Intranet IP(s) bound to the group

netmask The netmask for the Intranet IP

intranetIP6 The Intranet IP6(s) bound to the group

numaddr Numbers of ipv6 address bound starting with intranetip6

policySubType stateflag gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

type Bindpoint to which the policy is bound.

weight Weight of this group with respect to other configured aaa groups (lower the number higher the weight)

devno count

Example

```
show aaa group engg GroupName: engg
```

```
Bound AAA users:

UserName: joe

UserName: jane

Intranetip IP: 10.102.10.0      Netmask: 255.255.255.0
```

Done

aaa-kcdAccount

The following operations can be performed on "aaa-kcdAccount":

set| add| unset| rm| show| check|

set aaa kcdAccount

Set the KCD account information.

Synopsis

set aaa kcdAccount <kcdAccount>

Arguments

kcdAccount The name of the KCD account.

keytab The path to the keytab file. If specified other parameters in this command need not be given

realmStr Kerberos Realm.

delegatedUser Username that can perform kerberos constrained delegation.

kcdPassword Password for Delegated User.

usercert SSL Cert (including private key) for Delegated User.

cacert CA Cert for UserCert or when doing PKINIT backchannel.

userRealm Realm of the user

enterpriseRealm Enterprise Realm of the user. This should be given only in certain KDC deployments where KDC expects Enterprise username instead of Principal Name

serviceSPN Service SPN. When specified, this will be used to fetch kerberos tickets. If not specified, Citrix ADC will construct SPN using service fqdn

Example

set aaa kcdaccount my_kcd_acct -keytab /var/hiskcd.keytab The above command sets the keytab location for KCD account my_kcd_acct to /var/hiskcd.keytab

add aaa kcdAccount

Add a Kerberos constrained delegation account.

Synopsis

add aaa kcdAccount <kcdAccount> {-keytab <string>} {-realmStr <string>} {-delegatedUser <string>} {-kcdPassword } {-usercert <string>} {-cacert <string>}

Arguments

kcdAccount The name of the KCD account.

keytab The path to the keytab file. If specified other parameters in this command need not be given

realmStr Kerberos Realm.

delegatedUser Username that can perform kerberos constrained delegation.

kcdPassword Password for Delegated User.

usercert SSL Cert (including private key) for Delegated User.

cacert CA Cert for UserCert or when doing PKINIT backchannel.

userRealm Realm of the user

enterpriseRealm Enterprise Realm of the user. This should be given only in certain KDC deployments where KDC expects Enterprise username instead of Principal Name

serviceSPN Service SPN. When specified, this will be used to fetch kerberos tickets. If not specified, Citrix ADC will construct SPN using service fqdn

Example

add aaa kcdaccount my_kcd_acct -keytab /var/mykcd.keytab add aaa kcdaccount my_kcd_acct -keytab The above example adds a Kerberos constrained delegation account my_kcd_acct, with the keytab file located at /var/mykcd.keytab

unset aaa kcdAccount

Unset the KCD account information..Refer to the set aaa kcdAccount command for meanings of the arguments.

Synopsis

unset aaa kcdAccount <kcdAccount>

rm aaa kcdAccount

Remove the KCD account.

Synopsis

rm aaa kcdAccount <kcdAccount>

Arguments

kcdAccount The KCD account name.

show aaa kcdAccount

Display KCD accounts.

Synopsis

show aaa kcdAccount

Arguments

kcdAccount The KCD account name.

Output

keytab The path to the keytab file. If specified other parameters in this command need not be given

principle SPN extracted from keytab file.

kcdSPN Host SPN extracted from keytab file.

realmStr Kerberos Realm.

delegatedUser Username that can perform kerberos constrained delegation.

kcdPassword Password for Delegated User.

usercert SSL Cert (including private key) for Delegated User.

cacert CA Cert for UserCert or when doing PKINIT backchannel.

userRealm Realm of the user

enterpriseRealm Enterprise Realm of the user. This should be given only in certain KDC deployments where KDC expects Enterprise username instead of Principal Name

serviceSPN Service SPN. When specified, this will be used to fetch kerberos tickets. If not specified, Citrix ADC will construct SPN using service fqdn

stateflag devno count

Example

Example

> show aaa kcdaccount my_kcd_acct KcdAccount: my_kcd_acct Keytab: /var/mykcd.keytab Done

check aaa kcdAccount

Check Kerberos configuration.

Synopsis

check aaa kcdAccount -realmStr <string> -delegatedUser <string> -kcdPassword <string> -serviceSPN <string>

Arguments

realmStr Active Directory Domain

delegatedUser Service Account Name

kcdPassword Service Account Password

serviceSPN Service FQDN

userRealm Impersonate user

Example

check aaa kcdAccount -realmStr AAA.LOCAL -delegatedUser svc_iis3 -kcdPassword <password> -serviceSPN iis3.aaa.local -userRealm ak1

aaa-ldapParams

The following operations can be performed on "aaa-ldapParams":

unset| set| show|

unset aaa ldapParams

Use this command to remove aaa ldapParams settings.Refer to the set aaa ldapParams command for meanings of the arguments.

Synopsis

unset aaa ldapParams

set aaa ldapParams

Modifies the global configuration settings for the LDAP server. The settings that you specify are used for all SSL-VPN virtual servers unless you use authentication policies to create a configuration for a specific SSL-VPN virtual server.

Synopsis

set aaa ldapParams {-ldapBindDnPassword } [-groupSearchAttribute <string>]

Arguments

serverIP IP address of your LDAP server.

serverPort Port number on which the LDAP server listens for connections. Default value: 389 Minimum value: 1

authTimeout Maximum number of seconds that the Citrix ADC waits for a response from the LDAP server. Default value: 3 Minimum value: 1

ldapBase Base (the server and location) from which LDAP search commands should start. If the LDAP server is running locally, the default value of base is dc=netscaler, dc=com.

ldapBindDn Complete distinguished name (DN) string used for binding to the LDAP server.

ldapBindDnPassword Password for binding to the LDAP server.

ldapLoginName Name attribute that the Citrix ADC uses to query the external LDAP server or an Active Directory.

searchFilter String to be combined with the default LDAP user search string to form the value to use when executing an LDAP search. For example, the following values: vpnallowed=true, ldaploginame=""samaccount"" when combined with the user-supplied username ""bob"", yield the following LDAP search string: ""(&(vpnallowed=true)(samaccount=bob)""

groupAttrName Attribute name used for group extraction from the LDAP server.

subAttributeName Subattribute name used for group extraction from the LDAP server.

secType Type of security used for communications between the Citrix ADC and the LDAP server. For the PLAINTEXT setting, no encryption is required.

Possible values: PLAINTEXT, TLS, SSL Default value: TLS

svrType The type of LDAP server.

Possible values: AD, NDS Default value: AAA_LDAP_SERVER_TYPE_DEFAULT

ssoNameAttribute Attribute used by the Citrix ADC to query an external LDAP server or Active Directory for an alternative username. This alternative username is then used for single sign-on (SSO).

passwdChange Accept password change requests.

Possible values: ENABLED, DISABLED Default value: DISABLED

nestedGroupExtraction Queries the external LDAP server to determine whether the specified group belongs to another group.

Possible values: ON, OFF Default value: OFF

maxNestingLevel Number of levels up to which the system can query nested LDAP groups. Default value: 2 Minimum value: 2

groupNameIdentifier LDAP-group attribute that uniquely identifies the group. No two groups on one LDAP server can have the same group name identifier.

groupSearchAttribute LDAP-group attribute that designates the parent group of the specified group. Use this attribute to search for a group's parent group.

groupSearchSubAttribute LDAP-group subattribute that designates the parent group of the specified group. Use this attribute to search for a group's parent group.

groupSearchFilter Search-expression that can be specified for sending group-search requests to the LDAP server.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

Example

To configure authentication in the LDAP server running at 192.40.1.2: set aaa ldapparams -serverip 192.40.1.2 -ldapbase "dc=netscaler,dc=com" -ldapBindDN "cn=Manager,dc=netscaler,dc=com" -ldapBindDnPassword secret -ldaploginname uid

Related Commands

- set aaa parameter

show aaa ldapParams

Displays the current LDAP configuration on the Citrix ADC.

Synopsis

show aaa ldapParams

Arguments

Output

serverIP The IP address of the LDAP server.

serverPort Port number on which the LDAP server listens for connections.

authTimeout Maximum number of seconds that the Citrix ADC waits for a response from the LDAP server.

ldapBindDnPassword Password for binding to the LDAP server.

ldapBindDn The full distinguished name used to bind to the LDAP server.

ldapLoginName The name attribute used by the system to query the external LDAP server, or an Active Directory.

ldapBase The base or node where the ldapsearch should start. If the LDAP server is running locally, the default value of base is dc=netscaler, dc=com.

secType The communication type between the system and the LDAP server.

svrType LDAP server.

ssoNameAttribute The attribute used by the system to query the external LDAP server, or an Active Directory, for an alternate username to be used in Single Sign-On.

searchFilter The String to be combined with the default LDAP user search string to form the value. For example, vpnallowed=true with ldaploginame "samaccount" and the user-supplied username "bob" would yield the LDAP search string "(&(vpnallowed=true)(samaccount=bob)".

groupAttrName The Attribute name for group extraction from the LDAP server.

subAttributeName Subattribute name used for group extraction from the LDAP server.

groupAuthName To associate AAA users with an AAA group, use the command

```
"bind AAA group ... -username ...".
```

You can bind different policies to each AAA group. Use the command

```
"bind AAA group ... -policy ..."
```

passwdChange Accept password change requests.

nestedGroupExtraction Queries the external LDAP server to determine whether the specified group belongs to another group.

maxNestingLevel Number of levels up to which the system can query nested LDAP groups.

groupNameIdentifier LDAP-group attribute that uniquely identifies the group. No two groups on one LDAP server can have the same group name identifier.

groupSearchAttribute LDAP-group attribute that designates the parent group of the specified group. Use this attribute to search for a group's parent group.

groupSearchSubAttribute LDAP-group subattribute that designates the parent group of the specified group. Use this attribute to search for a group's parent group.

groupSearchFilter Search-expression that can be specified for sending group-search requests to the LDAP server.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

Example

> show aaa ldapparams Configured LDAP parameters Server IP: 127.0.0.1 Port: 389 Timeout: 1 BindDn: cn=Manager,dc=florazel,dc=com login: uid Base: dc=florazel,dc=com Secure Type: PLAINTEXT Done

aaa-otpparameter

The following operations can be performed on "aaa-otpparameter":

show| unset| set|

show aaa otpparameter

Displays the current AAA OTP global configuration.

Synopsis

show aaa otpparameter

Arguments

Output

encryption To encrypt otp secret in AD or not. Default value is OFF

maxOTPDevices Maximum number of otp devices user can register. Default value is 4. Max value is 255

Example

> show aaa otpparameter Configured AAA OTP parameters Max OTP device Configured: 6 Done

unset aaa otpparameter

Use this command to remove aaa otpparameter settings.Refer to the set aaa otpparameter command for meanings of the arguments.

Synopsis

unset aaa otpparameter

set aaa otpparameter

Sets the global AAA OTP configuration.

Synopsis

set aaa otpparameter

Arguments

encryption To encrypt otp secret in AD or not. Default value is OFF

Possible values: ON, OFF Default value: OFF

maxOTPDevices Maximum number of otp devices user can register. Default value is 4. Max value is 255 Default value: 4 Minimum value: 0 Maximum value: 255

Example

set aaa otpparameter -maxotpdevice 6

aaa-parameter

The following operations can be performed on "aaa-parameter":

set| show| unset|

set aaa parameter

Sets the global AAA configuration. Any configuration settings made at this level overrides configuration settings for the authentication server.

Synopsis

set aaa parameter [-maxLoginAttempts <positive_integer>]

Arguments

enableStaticPageCaching The default state of VPN Static Page caching. Static Page caching is enabled by default.

Possible values: YES, NO Default value: YES

enableEnhancedAuthFeedback Enhanced auth feedback provides more information to the end user about the reason for an authentication failure. The default value is set to NO.

Possible values: YES, NO Default value: NO

defaultAuthType The default authentication server type.

Possible values: LOCAL, LDAP, RADIUS, TACACS, CERT Default value: LOCAL

maxAAAUsers Maximum number of concurrent users allowed to log on to VPN simultaneously. Minimum value: 1

maxLoginAttempts Maximum Number of login Attempts Minimum value: 1

failedLoginTimeout Number of minutes an account will be locked if user exceeds maximum permissible attempts Minimum value: 1 Maximum value: 525600

aaadnatIp Source IP address to use for traffic that is sent to the authentication server.

enableSessionStickiness Enables/Disables stickiness to authentication servers

Possible values: YES, NO Default value: NO

aaaSessionLoglevel Audit log level, which specifies the types of events to log for cli executed commands. Available values function as follows:

- EMERGENCY - Events that indicate an immediate crisis on the server.
- ALERT - Events that might require action.
- CRITICAL - Events that indicate an imminent server crisis.

- ERROR - Events that indicate some type of error.
- WARNING - Events that require action in the near future.
- NOTICE - Events that the administrator should know about.
- INFORMATIONAL - All but low-level events.
- DEBUG - All events, in extreme detail.

Possible values: EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG Default value: DEFAULT_LOGLEVEL_AAA

aaadLoglevel AAAD log level, which specifies the types of AAAD events to log in nsvpn.log. Available values function as follows:

- EMERGENCY - Events that indicate an immediate crisis on the server.
- ALERT - Events that might require action.
- CRITICAL - Events that indicate an imminent server crisis.
- ERROR - Events that indicate some type of error.
- WARNING - Events that require action in the near future.
- NOTICE - Events that the administrator should know about.
- INFORMATIONAL - All but low-level events.
- DEBUG - All events, in extreme detail.

Possible values: EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG Default value: INFORMATIONAL

dynAddr Set by the DHCP client when the IP address was fetched dynamically.

Possible values: ON, OFF Default value: OFF

ftMode First time user mode determines which configuration options are shown by default when logging in to the GUI. This setting is controlled by the GUI.

Possible values: ON, HA, OFF Default value: ON

maxSamlDeflateSize This will set the maximum deflate size in case of SAML Redirect binding. Minimum value: 0

persistentLoginAttempts Persistent storage of unsuccessful user login attempts

Possible values: ENABLED, DISABLED Default value: DISABLED

pwdExpiryNotificationDays This will set the threshold time in days for password expiry notification. Default value is 0, which means no notification is sent Minimum value: 0

maxKBQuestions This will set maximum number of Questions to be asked for KB Validation. Default value is 2, Max Value is 6 Minimum value: 2 Maximum value: 6

loginEncryption Parameter to encrypt login information for nFactor flow

Possible values: ENABLED, DISABLED Default value: DISABLED

SameSite SameSite attribute value for Cookies generated in AAATM context. This attribute value will be appended only for the cookies which are specified in the builtin patset ns_cookies_samesite

Possible values: None, LAX, STRICT

APITokenCache Option to enable/disable API cache feature.

Possible values: ENABLED, DISABLED Default value: DISABLED

tokenIntrospectionInterval Frequency at which a token must be verified at the Authorization Server (AS) despite being found in cache. Minimum value: 0

defaultCSPHeader Parameter to enable/disable default CSP header

Possible values: ENABLED, DISABLED Default value: DISABLED

httpOnlyCookie Parameter to set/reset HttpOnly Flag for NSC_AAAC/NSC_TMAS cookies in nfactor

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set aaa parameter -defaultAuthType RADIUS -maxAAAUSers 100

show aaa parameter

Displays the current AAA global configuration.

Synopsis

show aaa parameter

Arguments

Output

enableStaticPageCaching Indicates if static page caching is enabled or not.

enableEnhancedAuthFeedback Indicates whether enhanced auth feedback is enabled or not.

defaultAuthType The default authentication server type.

maxAAAUsers The maximum number of concurrent users allowed to log into the system at any time.

aaadnatIp The natIp to be used for the AAA traffic

maxLoginAttempts Maximum Number of login Attempts

failedLoginTimeout Number of minutes an account will be locked if user exceeds maximum permissible attempts

enableSessionStickiness Enables/Disables stickiness to authentication servers

aaaSessionLoglevel Audit log level, which specifies the types of events to log for cli executed commands. Available values function as follows:

- EMERGENCY - Events that indicate an immediate crisis on the server.
- ALERT - Events that might require action.
- CRITICAL - Events that indicate an imminent server crisis.
- ERROR - Events that indicate some type of error.
- WARNING - Events that require action in the near future.
- NOTICE - Events that the administrator should know about.
- INFORMATIONAL - All but low-level events.
- DEBUG - All events, in extreme detail.

aaadLoglevel AAAD log level, which specifies the types of AAAD events to log in nsvpn.log. Available values function as follows:

- EMERGENCY - Events that indicate an immediate crisis on the server.
- ALERT - Events that might require action.
- CRITICAL - Events that indicate an imminent server crisis.
- ERROR - Events that indicate some type of error.
- WARNING - Events that require action in the near future.

- NOTICE - Events that the administrator should know about.
- INFORMATIONAL - All but low-level events.
- DEBUG - All events, in extreme detail.

dynAddr Set by the DHCP client when the IP address was fetched dynamically.

ftMode First time user mode determines which configuration options are shown by default when logging in to the GUI. This setting is controlled by the GUI.

maxSamlDeflateSize This will set the maximum deflate size in case of SAML Redirect binding.

persistentLoginAttempts Persistent storage of unsuccessful user login attempts

pwdExpiryNotificationDays This will set the threshold time in days for password expiry notification. Default value is 0, which means no notification is sent

maxKBQuestions This will set maximum number of Questions to be asked for KB Validation. Default value is 2, Max Value is 6

builtin Flag to determine if aaa param is built-in or not

feature The feature to be checked while applying this config

loginEncryption Parameter to encrypt login information for nFactor flow

SameSite SameSite attribute value for Cookies generated in AAATM context. This attribute value will be appended only for the cookies which are specified in the builtin patset ns_cookies_samesite

APITokenCache Option to enable/disable API cache feature.

tokenIntrospectionInterval Frequency at which a token must be verified at the Authorization Server (AS) despite being found in cache.

defaultCSPHeader Parameter to enable/disable default CSP header

httpOnlyCookie Parameter to set/reset HttpOnly Flag for NSC_AAAC/NSC_TMAS cookies in nfactor

Example

> show aaa parameter Configured AAA parameters DefaultAuthType: LDAP MaxAAAUsers: 5 Done

unset aaa parameter

Resets the global AAA parameter settings on the Citrix ADC. Attributes for which a default value is available revert to their default values. See the set aaa parameter command for descriptions of the parameters..Refer to the set aaa parameter command for meanings of the arguments.

Synopsis

unset aaa parameter

aaa-preauthenticationaction

The following operations can be performed on "aaa-preauthenticationaction":

show| rm| unset| set| add|

show aaa preauthenticationaction

Displays details of the specified preauthentication action.

Synopsis

show aaa preauthenticationaction

Arguments

name Name of the preauthentication action.

Output

preauthenticationaction Allow or deny logon after endpoint analysis (EPA) results.

killProcess String specifying the name of a process to be terminated by the endpoint analysis (EPA) tool.

deletefiles String specifying the path(s) and name(s) of the files to be deleted by the endpoint analysis (EPA) tool.

stateflag builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

defaultEPAGroup This is the default group that is chosen when the EPA check succeeds.

devno count

rm aaa preauthenticationaction

Removes a preauthentication action. NOTE: A preauthentication action cannot be removed if it is bound to a policy.

Synopsis

rm aaa preauthenticationaction <name>

Arguments

name Name of the preauthentication action to remove.

unset aaa preauthenticationaction

Use this command to remove aaa preauthenticationaction settings.Refer to the set aaa preauthenticationaction command for meanings of the arguments.

Synopsis

unset aaa preauthenticationaction <name>

set aaa preauthenticationaction

Modifies an existing preauthentication action (profile).

Synopsis

set aaa preauthenticationaction <name>

Arguments

name Name of the preauthentication action to modify.

preauthenticationaction Allow or deny logon after endpoint analysis (EPA) results.

Possible values: ALLOW, DENY

killProcess String specifying the name of a process to be terminated by the endpoint analysis (EPA) tool.

deletefiles String specifying the path(s) and name(s) of the files to be deleted by the endpoint analysis (EPA) tool.

defaultEPAGroup This is the default group that is chosen when the EPA check succeeds. Maximum value: 64

add aaa preauthenticationaction

Adds an action (profile) for endpoint analysis (EPA) clients before authentication.

Synopsis

add aaa preauthenticationaction <name>

Arguments

name Name for the preauthentication action. Must begin with a letter, number, or the underscore character (_), and must consist only of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after preauthentication action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my aaa action" or 'my aaa action').

preauthenticationaction Allow or deny logon after endpoint analysis (EPA) results.

Possible values: ALLOW, DENY

killProcess String specifying the name of a process to be terminated by the endpoint analysis (EPA) tool.

deletefiles String specifying the path(s) and name(s) of the files to be deleted by the endpoint analysis (EPA) tool.

defaultEPAGroup This is the default group that is chosen when the EPA check succeeds. Maximum value: 64

aaa-preauthenticationparameter

The following operations can be performed on "aaa-preauthenticationparameter":

unset| set| show|

unset aaa preauthenticationparameter

Resets the default end point analysis(EPA) configuration settings on the Citrix ADC. Attributes for which a default value is available revert to their default values. See the set aaa preauthenticationparameter command for descriptions of the parameters..Refer to the set aaa preauthenticationparameter command for meanings of the arguments.

Synopsis

unset aaa preauthenticationparameter

set aaa preauthenticationparameter

Configures the default end point analysis (EPA) parameters that are applied before authentication.

Synopsis

set aaa preauthenticationparameter

Arguments

preauthenticationaction Deny or allow login on the basis of end point analysis results.

Possible values: ALLOW, DENY

rule Name of the Citrix ADC named rule, or an expression, to be evaluated by the EPA tool.

killProcess String specifying the name of a process to be terminated by the EPA tool.

deletefiles String specifying the path(s) to and name(s) of the files to be deleted by the EPA tool, as a string of between 1 and 1023 characters.

show aaa preauthenticationparameter

Displays the current preauthentication configuration.

Synopsis

show aaa preauthenticationparameter

Arguments

Output

preauthenticationaction Deny or allow login after End point analysis results.

rule Name of the Citrix ADC named rule, or an expression, to be evaluated by the EPA tool.

killProcess Processes to be killed by EPA tool.

deletefiles Files to be deleted by EPA tool.

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

aaa-preauthenticationpolicy

The following operations can be performed on "aaa-preauthenticationpolicy":

rm| set| show| add|

rm aaa preauthenticationpolicy

Removes the specified preauthentication policy.

Synopsis

rm aaa preauthenticationpolicy <name>

Arguments

name Name of the preauthentication policy to remove.

set aaa preauthenticationpolicy

Modifies the Request Action of a preauthentication policy.

Synopsis

set aaa preauthenticationpolicy <name>

Arguments

name Name of the preauthentication policy to modifiy.

rule The new rule to be associated with the policy.

reqAction Name of the action that the policy is to invoke when a connection matches the policy.

show aaa preauthenticationpolicy

Displays the properties of either the specified preauthentication policy or (if none is specified) a list of all configured preauthentication policies.

Synopsis

show aaa preauthenticationpolicy

Arguments

name Name of the preauthentication policy whose properties you want to view.

Output

rule The new rule associated with the policy.

reqAction The Pre-authentication action associated with the policy.

hits No of hits.

boundTo The entity name to which policy is bound

activePolicy priority bindPolicyType policyType builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

devno count stateflag

add aaa preauthenticationpolicy

Adds a preauthentication policy. The policy defines expressions to be evaluated by the endpoint analysis (EPA) tool.

Synopsis

add aaa preauthenticationpolicy <name> <rule>

Arguments

name Name for the preauthentication policy. Must begin with a letter, number, or the underscore character (_), and must consist only of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the preauthentication policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

rule Name of the Citrix ADC named rule, or an expression, defining connections that match the policy.

reqAction Name of the action that the policy is to invoke when a connection matches the policy.

aaa-radiusParams

The following operations can be performed on "aaa-radiusParams":

show| set| unset|

show aaa radiusParams

Displays the current RADIUS configuration on the Citrix ADC.

Synopsis

show aaa radiusParams

Arguments

Output

serverIP IP address of your RADIUS server.

serverPort Port number on which the RADIUS server listens for connections.

radKey The key shared between the RADIUS server and clients. Required for allowing the Citrix ADC to communicate with the RADIUS server.

groupAuthName To associate AAA users with an AAA group, use the command

```
"bind AAA group ... -username ...".
```

You can bind different policies to each AAA group. Use the command

```
"bind AAA group ... -policy ..."
```

authTimeout Maximum number of seconds that the Citrix ADC waits for a response from the RADIUS server.

radNASip The option to send the Citrix ADC's IP address (NSIP) as the "nasip" (Network Access Server IP) part of the Radius protocol to the server.

radNASid The nasid (Network Access Server ID). If configured, this string will be sent to the RADIUS server as the "nasid" as part of the Radius protocol.

IPAddress IP Address.

radVendorID Vendor ID for RADIUS group extraction.

radAttributeType Attribute type for RADIUS group extraction.

radGroupsPrefix Prefix string that precedes group names within a RADIUS attribute for RADIUS group extraction.

radGroupSeparator Group separator string that delimits group names within a RADIUS attribute for RADIUS group extraction.

passEncoding Enable password encoding in RADIUS packets that the Citrix ADC sends to the RADIUS server.

ipVendorID Vendor ID attribute in the RADIUS response. If the attribute is not vendor-encoded, it is set to 0.

ipAttributeType IP attribute type in the RADIUS response.

accounting The state of the Radius server that will receive accounting messages.

pwdVendorID Vendor ID of the password in the RADIUS response. Used to extract the user password.

pwdAttributeType Attribute type of the Vendor ID in the RADIUS response.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

callingstationid Send Calling-Station-ID of the client to the RADIUS server. IP Address of the client is sent as its Calling-Station-ID.

authservRetry Number of retry by the Citrix ADC before getting response from the RADIUS server.

authentication Configure the RADIUS server state to accept or refuse authentication messages.

tunnelEndpointClientIP Send Tunnel Endpoint Client IP address to the RADIUS server.

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

Example

> show aaa radiusparams Configured RADIUS parameters Server IP: 127.0.0.2 Port: 1812 key: secret Timeout: 10 Done

set aaa radiusParams

Modifies the global configuration settings for the RADIUS server. The settings that you specify are used for all SSL-VPN virtual servers unless you use authentication policies to create a configuration for a specific SSL-VPN virtual server.

Synopsis

set aaa radiusParams {-radKey }

Arguments

serverIP IP address of your RADIUS server.

serverPort Port number on which the RADIUS server listens for connections. Default value: 1812 Minimum value: 1

authTimeout Maximum number of seconds that the Citrix ADC waits for a response from the RADIUS server. Default value: 3 Minimum value: 1

radKey The key shared between the RADIUS server and clients. Required for allowing the Citrix ADC to communicate with the RADIUS server.

radNASip Send the Citrix ADC IP (NSIP) address to the RADIUS server as the Network Access Server IP (NASIP) part of the Radius protocol.

Possible values: ENABLED, DISABLED

radNASid Send the Network Access Server ID (NASID) for your Citrix ADC to the RADIUS server as the nasid part of the Radius protocol.

radVendorID Vendor ID for RADIUS group extraction. Minimum value: 1

radAttributeType Attribute type for RADIUS group extraction. Minimum value: 1

radGroupsPrefix Prefix string that precedes group names within a RADIUS attribute for RADIUS group extraction.

radGroupSeparator Group separator string that delimits group names within a RADIUS attribute for RADIUS group extraction.

passEncoding Enable password encoding in RADIUS packets that the Citrix ADC sends to the RADIUS server.

Possible values: pap, chap, mschapv1, mschapv2 Default value: mschapv2

ipVendorID Vendor ID attribute in the RADIUS response. If the attribute is not vendor-encoded, it is set to 0. Minimum value: 0

ipAttributeType IP attribute type in the RADIUS response. Minimum value: 1

accounting Configure the RADIUS server state to accept or refuse accounting messages.

Possible values: ON, OFF

pwdVendorID Vendor ID of the password in the RADIUS response. Used to extract the user password. Minimum value: 1

pwdAttributeType Attribute type of the Vendor ID in the RADIUS response. Minimum value: 1

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

callingstationid Send Calling-Station-ID of the client to the RADIUS server. IP Address of the client is sent as its Calling-Station-ID.

Possible values: ENABLED, DISABLED Default value: DISABLED

authservRetry Number of retry by the Citrix ADC before getting response from the RADIUS server. Default value: 3 Minimum value: 1 Maximum value: 10

authentication Configure the RADIUS server state to accept or refuse authentication messages.

Possible values: ON, OFF Default value: ON

tunnelEndpointClientIP Send Tunnel Endpoint Client IP address to the RADIUS server.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

To configure the default RADIUS parameters: set aaa radiusparams -serverip 192.30.1.2 -radkey sslvpn

Related Commands

- set aaa parameter

unset aaa radiusParams

Use this command to remove aaa radiusParams settings.Refer to the set aaa radiusParams command for meanings of the arguments.

Synopsis

unset aaa radiusParams

aaa-session

The following operations can be performed on "aaa-session":

show| kill|

show aaa session

Displays all AAA-TM/VPN connections that are bound to the specified user, group, IP address, or IP range.

Synopsis

show aaa session [-intranetIP <ip_addr|*>]

Arguments

userName Name of the AAA user.

groupName Name of the AAA group.

intranetIP IP address or the first address in the intranet IP range.

netmask Subnet mask for the intranet IP range.

sessionKey Show aaa session associated with given session key

Output

publicIP Client's public IP address

publicPort Client's public port

IPAddress Citrix ADC's IP address

port Citrix ADC's port

privateIP Client's private/mapped IP address

privatePort Client's private/mapped port

destIP Destination IP address

destPort Destination port

intranetIP Specifies the Intranet IP

intranetIP6 Specifies the Intranet IP6

peId Core id of the session owner

stateflag devno count

Example

```
show aaa session clientIp (ClientPort) -> ServerIp(ServerPort)
```

```
PE id : 0
```

User name: user1 Session Type: TMSession Key: ****

10.101.1.56 (65223) -> 10.106.190.177 (80) PE 1 Done

kill aaa session

Terminates the specified AAA-TM/VPN session.

Synopsis

kill aaa session [-intranetIP <ip_addr|*>]

Arguments

userName Terminate AAA-TM/VPN sessions that belong to the specified user.

groupName Terminate AAA-TM/VPN sessions that belong to any user that is a member of the specified group.

intranetIP Terminate AAA-TM/VPN sessions that are associated with the specified intranet IP address or with an address in the range specified by the address and subnet mask.

netmask When terminating AAA-TM/VPN sessions that are associated with an IP address range, the subnet mask defining the range.

sessionKey Show aaa session associated with given session key

all Terminate all active AAA-TM/VPN sessions.

Example

kill aaa session -user joe

aaa-ssoprofile

The following operations can be performed on "aaa-ssoprofile":

rm| show| set| add|

rm aaa ssoprofile

Removes a SSO Profile from the appliance.

Synopsis

rm aaa ssoprofile <name>

Arguments

name Name of the SSOProfile to remove.

show aaa ssoprofile

Displays information about all SSO Profiles configured on the appliance.

Synopsis

show aaa ssoprofile

Arguments

name Name of the SSOProfile about which to display information.

Output

userName Name for the user. Must begin with a letter, number, or the underscore (_) character, and must contain only alphanumeric, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), and underscore characters.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my group" or 'my group').

password Password with which the user logs on. Required for Single sign on to external server.

devno count stateflag

set aaa ssoprofile

Modifies the specified parameters of a SSOProfile

Synopsis

set aaa ssoprofile <name>

Arguments

name Name of SSOProfile to be modified.

userName Name for the user. Must begin with a letter, number, or the underscore (_) character, and must contain only alphanumeric, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), and underscore characters.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my group" or 'my group').

password Password with which the user logs on. Required for Single sign on to external server.

add aaa ssoprofile

Creates a SSOProfile.

Synopsis

add aaa ssoprofile <name> -userName <string> -password

Arguments

name Name for the SSO Profile. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after a SSO Profile is created.

The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

userName Name for the user. Must begin with a letter, number, or the underscore (_) character, and must contain only alphanumeric, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), and underscore characters.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my group" or 'my group').

password Password with which the user logs on. Required for Single sign on to external server.

aaa-stats

The following operations can be performed on "aaa-stats":

show aaa stats

show aaa stats is an alias for stat aaa

Synopsis

show aaa stats - alias for 'stat aaa'

aaa-tacacsParams

The following operations can be performed on "aaa-tacacsParams":

unset| set| show|

unset aaa tacacsParams

Use this command to remove aaa tacacsParams settings.Refer to the set aaa tacacsParams command for meanings of the arguments.

Synopsis

unset aaa tacacsParams

set aaa tacacsParams

Modifies the global configuration settings for the TACACS+ server. The settings that you specify are used for all SSL-VPN virtual servers unless you use authentication policies to create a configuration for a specific SSL-VPN virtual server.

Synopsis

set aaa tacacsParams {-tacacsSecret }

Arguments

serverIP IP address of your TACACS+ server.

serverPort Port number on which the TACACS+ server listens for connections. Default value: 49 Minimum value: 1

authTimeout Maximum number of seconds that the Citrix ADC waits for a response from the TACACS+ server. Default value: 3 Minimum value: 1

tacacsSecret Key shared between the TACACS+ server and clients. Required for allowing the Citrix ADC to communicate with the TACACS+ server.

authorization Use streaming authorization on the TACACS+ server.

Possible values: ON, OFF

accounting Send accounting messages to the TACACS+ server.

Possible values: ON, OFF

auditFailedCmds The option for sending accounting messages to the TACACS+ server.

Possible values: ON, OFF

groupAttrName TACACS+ group attribute name.Used for group extraction on the TACACS+ server.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

Example

To configure a TACACS+ server running at 192.168.1.20 set aaa tacacsparams -serverip 192.168.1.20 -tacacssecret secret

Related Commands

- set aaa parameter

show aaa tacacsParams

Displays the Citrix ADC's current AAA TACACS+ configuration.

Synopsis

show aaa tacacsParams

Arguments

Output

serverIP IP address of your TACACS+ server.

serverPort Port number on which the TACACS+ server listens for connections.

authTimeout Maximum number of seconds that the Citrix ADC waits for a response from the TACACS+ server.

tacacsSecret The key shared between the client and the server.

authorization The option for the streaming authorization for TACACS+ server.

accounting The option to send accounting messages to TACACS+ server.

auditFailedCmds The option to send accounting messages to TACACS+ server.

groupAttrName TACACS+ group attribute name.Used for group extraction on the TACACS+ server.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

Example

> sh aaa tacacsparams Configured TACACS parameter Server IP: 192.168.1.20 Port: 49 Timeout: 1 secs Done

aaa-user

The following operations can be performed on "aaa-user":

lock| unbind| rm| show| bind| set| add| unlock|

lock aaa user

Locks a AAA user account for 24 hours unless it is explicitly unlocked by unlock aaa user .

Synopsis

lock aaa user <userName>

Arguments

userName Name of the AAA user account to lock.

unbind aaa user

Unbinds a policy from the specified user account.

Synopsis

unbind aaa user <userName> [-policy <string>] [-intranetIP <ip_addr>] [-intranetIP6 <ip_addr|ipv6_addr|*>]

Arguments

userName Name of the user account from which to unbind the policy.

policy Name of the policy to unbind.

type Bindpoint to which the policy is bound.

Possible values: REQUEST, UDP_REQUEST, DNS_REQUEST, ICMP_REQUEST Default value: REQUEST

intranetApplication Name of the intranet VPN application from which you are unbinding the policy.

urlName URL of the intranet application from which you are unbinding the policy.

intranetIP Intranet IP address of the application from which you are unbinding the policy.

netmask Subnet mask for the IP range in which the intranet application from which you are unbinding the policy resides. Required if the intranet application has multiple IP addresses bound to it. Not needed if the intranet application resides on a single IP address.

intranetIP6 IP6 address of the intranet application to which you are binding the policy.

numaddr Number of addresses for the IPv6 range in which the intranet application to which you are binding the policy resides. Required if the intranet application has multiple IPv6 addresses bound to it. Not needed if the intranet application resides on a single IP address. Minimum value: 1

Example

unbind AAA user joe -intranetip 10.102.1.123

rm aaa user

Removes a local AAA user account and the associated configuration.

Synopsis

rm aaa user <userName>

Arguments

userName Name of the AAA user account to remove.

show aaa user

Displays the current configuration of a AAA user account.

Synopsis

show aaa user

Arguments

userName Name of the user who has the account.

loggedIn Show whether the user is logged in or not.

Output

groupName The group name

policy The policy Name.

priority Integer specifying the priority of the policy. A lower number indicates a higher priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies max priority is 64000.

intranetApplication Name of the intranet VPN application to which the policy applies.

urlName The intranet url.

actType intranetIP The Intranet IP bound to the user

netmask The netmask for the Intranet IP

intranetIP6 The Intranet IP6 bound to the user

numaddr Numbers of ipv6 address bound starting with intranetip6

policySubType stateflag password Password with which the user logs on. Required for any user account that does not exist on an external authentication server. If you are not using an external authentication server, all user accounts must have a password. If you are using an external authentication server, you must provide a password for local user accounts that do not exist on the authentication server.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

type Bindpoint to which the policy is bound.

devno count

Example

Example

```
show aaa user joe UserName: joe IntranetIP: 10.102.1.123
```

```
Bound to groups:

        GroupName: engg
```

Done

bind aaa user

Binds a policy to the specified user account.

Synopsis

bind aaa user <userName> [-policy <string>] [-intranetIP <ip_addr>] [-intranetIP6 <ip_addr|ipv6_addr|*>]

Arguments

userName User account to which to bind the policy.

policy Name for the policy that you are creating. Must begin with a letter, number, or the underscore character (_), and must consist only of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the policy is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or "my policy").

priority Integer specifying the priority of the policy. A lower number indicates a higher priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies max priority is 64000. Minimum value: 0 Maximum value: 2147483647

type Bindpoint to which the policy is bound.

Possible values: REQUEST, UDP_REQUEST, DNS_REQUEST, ICMP_REQUEST Default value: REQUEST

intranetApplication Name of the intranet VPN application to which the policy applies.

urlName URL of the intranet application to which you are binding the policy.

intranetIP IP address of the intranet application to which you are binding the policy.

netmask Subnet mask for the IP range in which the intranet application to which you are binding the policy resides. Required if the intranet application has multiple IP addresses bound to it. Not needed if the intranet application resides on a single IP address.

gotoPriorityExpression Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

intranetIP6 IP6 address of the intranet application to which you are binding the policy.

numaddr Number of addresses for the IPv6 range in which the intranet application to which you are binding the policy resides. Required if the intranet application has multiple IPv6 addresses bound to it. Not needed if the intranet application resides on a single IPv6 address. Minimum value: 1

Example

To bind intranetip to the user joe: bind aaa user joe -intranetip 10.102.1.123

set aaa user

Configures the password for an existing local AAA user account. This command prompts you for a new password. NOTE: AAA does not request confirmation of the new password, so you might want to test the new password before sending it to the user.

Synopsis

set aaa user <userName>

Arguments

userName Name of the local AAA user account.

password Password with which the user logs on. Required for any user account that does not exist on an external authentication server. If you are not using an external authentication server, all user accounts must have a password. If you are using an external authentication server, you must provide a password for local user accounts that do not exist on the authentication server.

Example

set aaa user johndoe password abcd The above command sets the password for johndoe to abcd

add aaa user

Adds a local AAA user account and verifies the configuration to ensure that it is correct.

Synopsis

add aaa user <userName> {-password }

Arguments

userName Name for the user. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the user is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my aaa user" or "my aaa user").

password Password with which the user logs on. Required for any user account that does not exist on an external authentication server. If you are not using an external authentication server, all user accounts must have a password. If you are using an external authentication server, you must provide a password for local user accounts that do not exist on the authentication server.

Example

add aaa user johndoe -password abcd add aaa user johndoe -password The above example adds user johndoe with password abcd for first case, password supplied on prompt for second case

unlock aaa user

Unlocks a AAA user account which has been locked earlier for exceeding login attempts.

Synopsis

unlock aaa user <userName>

Arguments

userName Name of the AAA user account to unlock.

aaa

The following operations can be performed on "aaa":

stat aaa

Display aaa statistics

Synopsis

stat aaa

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Authentication successes (authsucc) Count of authentication successes.

Authentication failures (authfails) Count of authentication failures.

HTTP authorization successes (atzhtps) Count of HTTP connections that succeeded authorization.

HTTP authorization failures (atzhtpf) Count of HTTP connections that failed authorization.

Non HTTP authorization successes (atznonhtps) Count of non HTTP connections that succeeded authorization.

Non HTTP authorization failures (atznonhtpf) Count of non HTTP connections that failed authorization.

Current SmartAccess AAA Sessions (totcursess) Count of current SmartAccess AAA sessions.

Total SmartAccess AAA sessions (totsess) Count of all SmartAccess AAA sessions.

Timed out AAA sessions (totsessto) Count of AAA sessions that have timed out.

Current Basic (ICAOnly) AAA Sess (totcuricasess) Count of current Basic ICA only sessions.

Current Basic (ICAOnly) ICA Conn (curicaonlyconn) Count of current Basic ICA only connections.

Current Smart Access ICA Conn (curicaconn) Count of current SmartAccess ICA connections.

Current TM sessions (curTMses) Count of current AAATM sessions.

TM sessions (totTMses) Count of all AAATM sessions.

adm

Adm

The entities on which you can perform NetScaler CLI operations:

adm-parameter

The following operations can be performed on "adm-parameter":

unset| show| set|

unset adm parameter

Use this command to remove adm parameter settings.Refer to the set adm parameter command for meanings of the arguments.

Synopsis

unset adm parameter -admserviceconnect

show adm parameter

Displays the ADM parameters.

Synopsis

show adm parameter

Arguments

Output

admserviceconnect Parameter to enable/disable Citrix ADM Service Connect. This feature helps you discover your Citrix ADC instances effortlessly on Citrix ADM service and get insights and curated machine learning based recommendations for applications and Citrix ADC infrastructure. This feature lets the Citrix ADC instance automatically send system, usage and telemetry data to

Citrix ADM service. View here to learn more about this feature. Use of this feature is subject to the Citrix End User ServiceAgreement. View here

LowTouchOnboard ENABLED value indicates that this ADC can be on-boarded onto Citrix ADM Service using auto-onboarding process. Refer to for further details.

Example

show adm parameter

set adm parameter

Sets the ADM parameters.

Synopsis

set adm parameter -admserviceconnect (ENABLED | DISABLED)

Arguments

admserviceconnect Parameter to enable/disable Citrix ADM Service Connect. This feature helps you discover your Citrix ADC instances effortlessly on Citrix ADM service and get insights and curated machine learning based recommendations for applications and Citrix ADC infrastructure. This feature lets the Citrix ADC instance automatically send system, usage and telemetry data to Citrix ADM service. View here to learn more about this feature. Use of this feature is subject to the Citrix End User ServiceAgreement. View here

Possible values: ENABLED, DISABLED Default value: ENABLED

Example

set adm parameter -admserviceconnect (ENABLED|DISABLED)

analytics

Analytics

The entities on which you can perform NetScaler CLI operations:

analytics-global

The following operations can be performed on "analytics-global":

show| unbind| bind|

show analytics global

Displays the analytics profiles bound globally.

Synopsis

show analytics global

Arguments

Output

stateflag analyticsProfile Name of the analytics profile bound.

devno count

Example

show analytics global

unbind analytics global

Unbind analytics profile globally.

Synopsis

unbind analytics global <analyticsProfile>

Arguments

analyticsProfile Name of analytics profile being bound.

bind analytics global

Bind analytics profile globally.

Synopsis

bind analytics global <analyticsProfile>

Arguments

analyticsProfile Name of analytics profile being bound.

analytics-profile

The following operations can be performed on "analytics-profile":

add| rm| set| show| unset|

add analytics profile

Adds a new Analytics profile. A Profile Specifies what application insight is needed. Also specifies the collector to which the data needs to be exported. example => add analytics profile analytics_profile1 -collector 192.168.1.40 -type webinsight

Synopsis

add analytics profile <name> -type <type> [-outputMode <outputMode>]

Arguments

name Name for the analytics profile. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow profile" or 'my appflow profile').

collectors The collector can be an IP, an appflow collector name, a service or a vserver. If IP is specified, the transport is considered as logstream and default port of 5557 is taken. If collector name is specified, the collector properties are taken from the configured collector. If service is

specified, the configured service is assumed as the collector. If vserver is specified, the services bound to it are considered as collectors and the records are load balanced.

type This option indicates what information needs to be collected and exported.

Possible values: global, webinsight, tcpinsight, securityinsight, videoinsight, hdxinsight, gatewayinsight, timeseries, lsninsight, botinsight, CIinsight, udpinsight

httpClientSideMeasurements On enabling this option, the Citrix ADC will insert a javascript into the HTTP response to collect the client side page-timings and will send the same to the configured collectors.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpPageTracking On enabling this option, the Citrix ADC will link the embedded objects of a page together.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpURL On enabling this option, the Citrix ADC will log the URL in appflow records

Possible values: ENABLED, DISABLED Default value: DISABLED

httpHost On enabling this option, the Citrix ADC will log the Host header in appflow records

Possible values: ENABLED, DISABLED Default value: DISABLED

httpMethod On enabling this option, the Citrix ADC will log the method header in appflow records

Possible values: ENABLED, DISABLED Default value: DISABLED

httpReferer On enabling this option, the Citrix ADC will log the referer header in appflow records

Possible values: ENABLED, DISABLED Default value: DISABLED

httpUserAgent On enabling this option, the Citrix ADC will log User-Agent header.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpCookie On enabling this option, the Citrix ADC will log cookie header.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpLocation On enabling this option, the Citrix ADC will log location header.

Possible values: ENABLED, DISABLED Default value: DISABLED

urlCategory On enabling this option, the Citrix ADC will send the URL category record.

Possible values: ENABLED, DISABLED Default value: DISABLED

allHttpHeaders On enabling this option, the Citrix ADC will log all the request and response headers.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpContentType On enabling this option, the Citrix ADC will log content-length header.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpAuthentication On enabling this option, the Citrix ADC will log Authentication header.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpVia On enabling this option, the Citrix ADC will Via header.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpXForwardedForHeader On enabling this option, the Citrix ADC will log X-Forwarded-For header.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpSetCookie On enabling this option, the Citrix ADC will log set-cookie header.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpSetCookie2 On enabling this option, the Citrix ADC will log set-cookie2 header.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpDomainName On enabling this option, the Citrix ADC will log domain name.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpURLQuery On enabling this option, the Citrix ADC will log URL Query.

Possible values: ENABLED, DISABLED Default value: DISABLED

tcpBurstReporting On enabling this option, the Citrix ADC will log TCP burst parameters.

Possible values: ENABLED, DISABLED Default value: ENABLED

cqaReporting On enabling this option, the Citrix ADC will log TCP CQA parameters.

Possible values: ENABLED, DISABLED Default value: DISABLED

integratedCache On enabling this option, the Citrix ADC will log the Integrated Caching appflow records

Possible values: ENABLED, DISABLED Default value: DISABLED

grpcStatus On enabling this option, the Citrix ADC will log the gRPC status headers

Possible values: ENABLED, DISABLED Default value: DISABLED

outputMode This option indicates the format of REST API POST body. It depends on the consumer of the analytics data.

Possible values: avro, prometheus, influx Default value: avro,

metrics This option indicates the whether metrics should be sent to the REST collector.

Possible values: ENABLED, DISABLED Default value: DISABLED

events This option indicates the whether events should be sent to the REST collector.

Possible values: ENABLED, DISABLED Default value: DISABLED

auditlogs This option indicates the whether auditlog should be sent to the REST collector.

Possible values: ENABLED, DISABLED Default value: DISABLED

serveMode This option is for setting the mode of how data is provided

Possible values: Push, Pull Default value: Push

schemaFile This option is for configuring json schema file containing a list of counters to be exported by metricscollector Default value: NS_S_ANALYTICS_DEFAULT_SCHEMA_FILE Maximum value: 64

metricsExportFrequency This option is for configuring the metrics export frequency in seconds, frequency value must be in seconds range Default value: 30 Minimum value: 30 Maximum value: 300

analyticsAuthToken Token for authenticating with the endpoint. If the endpoint requires the Authorization header in a particular format, specify the complete format as the value to this parameter. For eg., in case of splunk, the Authorizaiton header is required to be of the form - Splunk <auth-token>. Maximum value: 256

analyticsEndpointUrl The URL at which to upload the analytics data on the endpoint Maximum value: 256

analyticsEndpointContentType By default, application/json content-type is used. If this needs to be overridden, specify the value. Maximum value: 128

analyticsEndpointMetadata If the endpoint requires some metadata to be present before the actual json data, specify the same. Maximum value: 128

rm analytics profile

Removes an Analytics profile.

Synopsis

rm analytics profile <name>

Arguments

name Name of the profile to remove.

Example

rm analytics profile analytics_profile1

set analytics profile

Sets an Analytics profile

Synopsis

set analytics profile <name>

Arguments

name Name for the analytics profile. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow profile" or 'my appflow profile').

collectors The collector can be an IP, an appflow collector name, a service or a vserver. If IP is specified, the transport is considered as logstream and default port of 5557 is taken. If collector

name is specified, the collector properties are taken from the configured collector. If service is specified, the configured service is assumed as the collector. If vserver is specified, the services bound to it are considered as collectors and the records are load balanced.

type This option indicates what information needs to be collected and exported.

Possible values: global, webinsight, tcpinsight, securityinsight, videoinsight, hdxinsight, gatewayinsight, timeseries, lsninsight, botinsight, CIinsight, udpinsight

httpClientSideMeasurements On enabling this option, the Citrix ADC will insert a javascript into the HTTP response to collect the client side page-timings and will send the same to the configured collectors.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpPageTracking On enabling this option, the Citrix ADC will link the embedded objects of a page together.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpURL On enabling this option, the Citrix ADC will log the URL in appflow records

Possible values: ENABLED, DISABLED Default value: DISABLED

httpHost On enabling this option, the Citrix ADC will log the Host header in appflow records

Possible values: ENABLED, DISABLED Default value: DISABLED

httpMethod On enabling this option, the Citrix ADC will log the method header in appflow records

Possible values: ENABLED, DISABLED Default value: DISABLED

httpReferer On enabling this option, the Citrix ADC will log the referer header in appflow records

Possible values: ENABLED, DISABLED Default value: DISABLED

httpUserAgent On enabling this option, the Citrix ADC will log User-Agent header.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpCookie On enabling this option, the Citrix ADC will log cookie header.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpLocation On enabling this option, the Citrix ADC will log location header.

Possible values: ENABLED, DISABLED Default value: DISABLED

urlCategory On enabling this option, the Citrix ADC will send the URL category record.

Possible values: ENABLED, DISABLED Default value: DISABLED

allHttpHeaders On enabling this option, the Citrix ADC will log all the request and response headers.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpContentType On enabling this option, the Citrix ADC will log content-length header.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpAuthentication On enabling this option, the Citrix ADC will log Authentication header.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpVia On enabling this option, the Citrix ADC will Via header.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpXForwardedForHeader On enabling this option, the Citrix ADC will log X-Forwarded-For header.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpSetCookie On enabling this option, the Citrix ADC will log set-cookie header.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpSetCookie2 On enabling this option, the Citrix ADC will log set-cookie2 header.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpDomainName On enabling this option, the Citrix ADC will log domain name.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpURLQuery On enabling this option, the Citrix ADC will log URL Query.

Possible values: ENABLED, DISABLED Default value: DISABLED

tcpBurstReporting On enabling this option, the Citrix ADC will log TCP burst parameters.

Possible values: ENABLED, DISABLED Default value: ENABLED

cqaReporting On enabling this option, the Citrix ADC will log TCP CQA parameters.

Possible values: ENABLED, DISABLED Default value: DISABLED

integratedCache On enabling this option, the Citrix ADC will log the Integrated Caching appflow records

Possible values: ENABLED, DISABLED Default value: DISABLED

grpcStatus On enabling this option, the Citrix ADC will log the gRPC status headers

Possible values: ENABLED, DISABLED Default value: DISABLED

outputMode This option indicates the format of REST API POST body. It depends on the consumer of the analytics data.

Possible values: avro, prometheus, influx Default value: avro,

metrics This option indicates the whether metrics should be sent to the REST collector.

Possible values: ENABLED, DISABLED Default value: DISABLED

events This option indicates the whether events should be sent to the REST collector.

Possible values: ENABLED, DISABLED Default value: DISABLED

auditlogs This option indicates the whether auditlog should be sent to the REST collector.

Possible values: ENABLED, DISABLED Default value: DISABLED

serveMode This option is for setting the mode of how data is provided

Possible values: Push, Pull Default value: Push

schemaFile This option is for configuring json schema file containing a list of counters to be exported by metricscollector Default value: NS_S_ANALYTICS_DEFAULT_SCHEMA_FILE Maximum value: 64

metricsExportFrequency This option is for configuring the metrics export frequency in seconds, frequency value must be in seconds range Default value: 30 Minimum value: 30 Maximum value: 300

analyticsAuthToken Token for authenticating with the endpoint. If the endpoint requires the Authorization header in a particular format, specify the complete format as the value to this

parameter. For eg., in case of splunk, the Authorizaiton header is required to be of the form - Splunk <auth-token>. Maximum value: 256

analyticsEndpointUrl The URL at which to upload the analytics data on the endpoint Maximum value: 256

analyticsEndpointContentType By default, application/json content-type is used. If this needs to be overridden, specify the value. Maximum value: 128

analyticsEndpointMetadata If the endpoint requires some metadata to be present before the actual json data, specify the same. Maximum value: 128

Example

set analytics profile analytics_profile1 -collector 1.2.3.4

show analytics profile

Displays information about all configured Analytics profiles, or about the specified profile.

Synopsis

show analytics profile

Arguments

name Name of the profile about which to display information.

Output

collectors The collector can be an IP, an appflow collector name, a service or a vserver. If IP is specified, the transport is considered as logstream and default port of 5557 is taken. If collector name is specified, the collector properties are taken from the configured collector. If service is specified, the configured service is assumed as the collector. If vserver is specified, the services bound to it are considered as collectors and the records are load balanced.

refCnt The number of references to the profile.

type This option indicates what information needs to be collected and exported.

httpClientSideMeasurements On enabling this option, the Citrix ADC will insert a javascript into the HTTP response to collect the client side page-timings and will send the same to the configured collectors.

httpPageTracking On enabling this option, the Citrix ADC will link the embedded objects of a page together.

httpURL On enabling this option, the Citrix ADC will log the URL in appflow records

httpHost On enabling this option, the Citrix ADC will log the Host header in appflow records

httpMethod On enabling this option, the Citrix ADC will log the method header in appflow records

httpReferer On enabling this option, the Citrix ADC will log the referer header in appflow records

httpUserAgent On enabling this option, the Citrix ADC will log User-Agent header.

httpCookie On enabling this option, the Citrix ADC will log cookie header.

httpLocation On enabling this option, the Citrix ADC will log location header.

urlCategory On enabling this option, the Citrix ADC will send the URL category record.

allHttpHeaders On enabling this option, the Citrix ADC will log all the request and response headers.

httpContentType On enabling this option, the Citrix ADC will log content-length header.

httpAuthentication On enabling this option, the Citrix ADC will log Authentication header.

httpVia On enabling this option, the Citrix ADC will Via header.

httpXForwardedForHeader On enabling this option, the Citrix ADC will log X-Forwarded-For header.

httpSetCookie On enabling this option, the Citrix ADC will log set-cookie header.

httpSetCookie2 On enabling this option, the Citrix ADC will log set-cookie2 header.

httpDomainName On enabling this option, the Citrix ADC will log domain name.

httpURLQuery On enabling this option, the Citrix ADC will log URL Query.

tcpBurstReporting On enabling this option, the Citrix ADC will log TCP burst parameters.

cqaReporting On enabling this option, the Citrix ADC will log TCP CQA parameters.

integratedCache On enabling this option, the Citrix ADC will log the Integrated Caching appflow records

grpcStatus On enabling this option, the Citrix ADC will log the gRPC status headers

outputMode This option indicates the format of REST API POST body. It depends on the consumer of the analytics data.

metrics This option indicates the whether metrics should be sent to the REST collector.

events This option indicates the whether events should be sent to the REST collector.

auditlogs This option indicates the whether auditlog should be sent to the REST collector.

serveMode This option is for setting the mode of how data is provided

schemaFile This option is for configuring json schema file containing a list of counters to be exported by metricscollector

httpBodyExport On enabling this option, ADC will export HTTP request and response body

metricsExportFrequency This option is for configuring the metrics export frequency in seconds, frequency value must be in seconds range

analyticsAuthToken Token for authenticating with the endpoint. If the endpoint requires the Authorization header in a particular format, specify the complete format as the value to this parameter. For eg., in case of splunk, the Authorizaiton header is required to be of the form - Splunk <auth-token>.

analyticsEndpointUrl The URL at which to upload the analytics data on the endpoint

analyticsEndpointContentType By default, application/json content-type is used. If this needs to be overridden, specify the value.

analyticsEndpointMetadata If the endpoint requires some metadata to be present before the actual json data, specify the same.

devno count stateflag

Example

show analytics profile prof1

unset analytics profile

Use this command to remove analytics profile settings.Refer to the set analytics profile command for meanings of the arguments.

Synopsis

unset analytics profile <name>

api

Api

The entities on which you can perform NetScaler CLI operations:

- api-spec
- api-specfile

api-spec

The following operations can be performed on "api-spec":

add| rm| show| update|

add api spec

Adds a specfile to memory. After it is bound to a profile it can be used for validations. In a high-availability configuration, the path to spec file must be the same on the primary and the secondary appliance.

Synopsis

add api spec <name> -file <string>

Arguments

name Name for the spec. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the spec is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my spec" or 'my spec').

file Name of and, optionally, path to the api spec file. The spec file should be present on the appliance's hard-disk drive or solid-state drive. Storing a spec file in any location other than the default might cause inconsistency in a high availability setup. /nsconfig/apispec/ is the default path.

type Input format of the spec file. The three formats supported by the appliance are: PROTO OAS/ Swagger GRAPHQL

Possible values: PROTO, OAS, GRAPHQL Default value: PROTO

Example

1)add api spec example_spec01 -file /nsconfig/apispec/example_spec01.proto -type PROTO The above command loads a spec file of type PROTO.

rm api spec

Removes all the spec, or the specified spec, from the appliance. The spec is removed only if it is not referenced by an app firewall profile.

Synopsis

rm api spec <name> ...

Arguments

name Name of the spec to remove.

Example

1)rm api spec example_spec01 The above command removes the spec example_spec01 from the system.

show api spec

Displays information about all the spec configured on the appliance, or displays detailed information about the specified spec.

Synopsis

show api spec

Arguments

name Name of the spec for which to show detailed information.

Output

file Name of and, optionally, path to the api spec file. The spec file should be present on the appliance's hard-disk drive or solid-state drive. Storing a spec file in any location other than the default might cause inconsistency in a high availability setup. /nsconfig/apispec/ is the default path.

type Input format of the spec file. The three formats supported by the appliance are: PROTO OAS/ Swagger GRAPHQL

specMethod API method used for display purposes

specEndpoint API endpoint (could be GRPC service, REST path) used for display purposes

specOptionMethod GRPC API option method: REST way to reach GRPC Service. One per service/method combination

specOptionEndpoint GRPC API option endpoint: REST way to reach GRPC Service. One per service/method combination

devno count stateflag

Example

1. An example of the output of the show api spec command is shown below: 2 configured specs: 1)Name: example_spec01 File: example_spec01.proto Type: PROTO 2)Name: example_spec02 File: example_spec02.oas Type: OAS
2. An example of the output of the show api spec example_spec01 command is shown below: Name: example_spec01 File: example_spec01.proto Type: PROTO
3. GRPS Method: SayHello GRPC Service: Greeter

update api spec

Updates the api spec with latest specfile. In a high availability configuration, the path to the specfile must be the same on the primary and secondary nodes.

Synopsis

update api spec <name> -file <string>

Arguments

name Name for the spec. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the spec is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my spec" or 'my spec').

file Name of and, optionally, path to the api spec file. The spec file should be present on the appliance's hard-disk drive or solid-state drive. Storing a spec file in any location other than the default might cause inconsistency in a high availability setup. /nsconfig/apispec/ is the default path.

type Input format of the spec file. The three formats supported by the appliance are: PROTO OAS/ Swagger GRAPHQL

Possible values: PROTO, OAS, GRAPHQL Default value: PROTO

Example

1)update api spec example_spec01 -file /nsconfig/apispec/example_spec01.proto -type PROTO
The above command loads a spec file of type PROTO.

api-specfile

The following operations can be performed on "api-specfile":

import| show| rm|

import api specfile

Imports a spec file to the Citrix ADC, assigns it a name, and stores it in the /nsconfig/apispec/ specfile folder. The folder is created if it does not exist.

Synopsis

import api specfile <name> <src>

Arguments

name Name to assign to the imported spec file. Must begin with an ASCII alphanumeric or underscore(_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

src URL specifying the protocol, host, and path, including file name, to the spec file to be imported. For example, http://www.example.com/spec_file. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

password

Example

import specfile my-specfile http://www.example.com/spec_file

show api specfile

Displays a list of all the imported spec file objects on the Citrix ADC.

Synopsis

show api specfile

Arguments

Output

name Name to assign to the imported spec file. Must begin with an ASCII alphanumeric or underscore(_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

src URL specifying the protocol, host, and path, including file name, to the spec file to be imported. For example, http://www.example.com/spec_file. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

devno count stateflag

Example

show api specfile

rm api specfile

Deletes the specified spec file.

Synopsis

rm api specfile <name>

Arguments

name Name to assign to the imported spec file. Must begin with an ASCII alphanumeric or underscore(_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),equals (=), and hyphen (-) characters. The following requirement

applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

Example

rm api specfile <name>

app

App

The entities on which you can perform NetScaler CLI operations:

application

The following operations can be performed on "application":

import| export| rm|

import application

Imports application configuration information from an AppExpert application template file. You can specify a deployment file along with the template file. A template file contains application and variable definitions. A deployment file contains information about the services, service groups, endpoints, and variables that were in the AppExpert application configuration at the time the template file was created. Before you use template and deployment files, make sure that they are present in the /nsconfig/nstemplates/applications/ and /nsconfig/nstemplates/applications/deployment_files directories, respectively. You can transfer the files from your local drive to those directories on the Citrix ADC by using either FTP or the Citrix ADC configuration utility. In the configuration utility, you can also import the files and create the application by using a single wizard (AppExpert > Applications > Import > AppExpert Template Wizard).

Synopsis

import application <apptemplateFilename>

Arguments

apptemplateFilename Name of the AppExpert application template file.

appname Name to assign to the application on the Citrix ADC. If you do not provide a name, the appliance assigns the application the name of the template file.

deploymentFilename Name of the deployment file.

Example

import app application sampleapp -apptemplatefilename sampleapp.xml -deploymentfilename deploy.xml

export application

Exports application configuration information to an AppExpert application template file. A deployment file is created along with the template file. The template file contains application and variable definitions. The deployment file contains information about the services, service groups, endpoints, and variables that are in the AppExpert application configuration. The template and deployment files are exported to the /nsconfig/nstemplates/applications/ and /nsconfig/nstemplates/applications/deployment_files directories, respectively. If you use the configuration utility, you can also export an application to your local hard drive.

Synopsis

export application <appname>

Arguments

appname Name of the AppExpert application whose configuration you want to export to a template file.

apptemplateFilename Name with which to save the template file. If you do not specify a name, the template file is saved with the name of the application.

deploymentFilename Name with which to save the deployment file. If you do not specify a name, a string consisting of an underscore and “deployment” (_deployment) is automatically appended to the name of the template file to create the name of the deployment file.

rm application

Remove application configuration information from a Citrix ADC device. You can specify an application name as input. All the configuration belonging to the specified application will be removed from the device.

Synopsis

rm application <appname>

Arguments

appname Name of the AppExpert application whose configuration you want to remove from the Citrix ADC.

appflow

appflow-action

The following operations can be performed on "appflow-action":

show| rename| unset| set| rm| unbind| bind| add|

show appflow action

Displays information about AppFlow action(s), or about the specified AppFlow action.

Synopsis

show appflow action

Arguments

name Name of the action about which to display information.

Output

stateflag hits The number of times the action has been taken.

collectors Name(s) of collector(s) to be associated with the AppFlow action.

clientSideMeasurements On enabling this option, the Citrix ADC will collect the time required to load and render the mainpage on the client.

pageTracking On enabling this option, the Citrix ADC will start tracking the page for waterfall chart by inserting a NS_ESNS cookie in the response.

webInsight On enabling this option, the Citrix ADC will send the webinsight records to the configured collectors.

securityInsight On enabling this option, the Citrix ADC will send the security insight records to the configured collectors.

botInsight On enabling this option, the Citrix ADC will send the bot insight records to the configured collectors.

CIInsight On enabling this option, the Citrix ADC will send the ContentInspection Insight records to the configured collectors.

videoAnalytics On enabling this option, the Citrix ADC will send the videoinsight records to the configured collectors.

distributionAlgorithm On enabling this option, the Citrix ADC will distribute records among the collectors. Else, all records will be sent to all the collectors.

MetricsLog If only the stats records are to be exported, turn on this option.

TransactionLog Log ANOMALOUS or ALL transactions

referenceCount The number of references to the action.

description Description of the action

comment Comments associated with the AppFlow action.

analyticsProfile Analytics profile to be bound to the appflow action

devno count

Example

1. show appflow action
2. show appflow action appflow_action_1

rename appflow action

Renames an AppFlow action.

Synopsis

rename appflow action <name>@ <newName>@

Arguments

name Existing name of the action.

newName New name for the AppFlow action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow action" or 'my appflow action').

Example

rename appflow action old_name new_name

unset appflow action

Use this command to remove appflow action settings.Refer to the set appflow action command for meanings of the arguments.

Synopsis

unset appflow action <name>

set appflow action

Modifies the specified parameters of an AppFlow action.

Synopsis

set appflow action <name>

Arguments

name Name of the action to be modified.

collectors Name(s) of collector(s) to be associated with the AppFlow action.

clientSideMeasurements On enabling this option, the Citrix ADC will collect the time required to load and render the mainpage on the client.

Possible values: ENABLED, DISABLED Default value: DISABLED

comment Any comments about this action. In the CLI, if including spaces between words, enclose the comment in quotation marks. (The quotation marks are not required in the configuration utility.)

pageTracking On enabling this option, the Citrix ADC will start tracking the page for waterfall chart by inserting a NS_ESNS cookie in the response.

Possible values: ENABLED, DISABLED Default value: DISABLED

webInsight On enabling this option, the Citrix ADC will send the webinsight records to the configured collectors.

Possible values: ENABLED, DISABLED Default value: ENABLED

securityInsight On enabling this option, the Citrix ADC will send the security insight records to the configured collectors.

Possible values: ENABLED, DISABLED Default value: DISABLED

botInsight On enabling this option, the Citrix ADC will send the bot insight records to the configured collectors.

Possible values: ENABLED, DISABLED Default value: DISABLED

CIInsight On enabling this option, the Citrix ADC will send the ContentInspection Insight records to the configured collectors.

Possible values: ENABLED, DISABLED Default value: DISABLED

videoAnalytics On enabling this option, the Citrix ADC will send the videoinsight records to the configured collectors.

Possible values: ENABLED, DISABLED Default value: DISABLED

distributionAlgorithm On enabling this option, the Citrix ADC will distribute records among the collectors. Else, all records will be sent to all the collectors.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set appflow action appflow_action_1 -collectors col1 col2 col3

rm appflow action

Removes a configured AppFlow action. You cannot remove an action that is associated with an AppFlow policy.

Synopsis

rm appflow action <name>

Arguments

name Name of the action to be removed.

Example

rm appflow action appflow_action_1

unbind appflow action

unbind an entity from AppFlow action

Synopsis

unbind appflow action <name> -analyticsProfile <string>

Arguments

name Name for the action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow action" or 'my appflow action').

analyticsProfile Name of analytics profile to be unbound to the appflow action.

Example

unbind appflow action <action-name> -analyticsProfile <analytics-profile-name>

bind appflow action

Bind an entity to AppFlow action

Synopsis

bind appflow action <name> -analyticsProfile <string>

Arguments

name Name for the action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow action" or 'my appflow action').

analyticsProfile Name of analytics profile to be bound to the appflow action.

Example

bind appflow action <action-name> -analyticsProfile <analytics-profile-name>

add appflow action

Creates an AppFlow action. The action can be associated with an AppFlow policy by using the add appflow policy command.

Synopsis

add appflow action <name> -collectors <string> ...

Arguments

name Name for the action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow action" or 'my appflow action').

collectors Name(s) of collector(s) to be associated with the AppFlow action.

clientSideMeasurements On enabling this option, the Citrix ADC will collect the time required to load and render the mainpage on the client.

Possible values: ENABLED, DISABLED Default value: DISABLED

pageTracking On enabling this option, the Citrix ADC will start tracking the page for waterfall chart by inserting a NS_ESNS cookie in the response.

Possible values: ENABLED, DISABLED Default value: DISABLED

webInsight On enabling this option, the Citrix ADC will send the webinsight records to the configured collectors.

Possible values: ENABLED, DISABLED Default value: ENABLED

securityInsight On enabling this option, the Citrix ADC will send the security insight records to the configured collectors.

Possible values: ENABLED, DISABLED Default value: DISABLED

botInsight On enabling this option, the Citrix ADC will send the bot insight records to the configured collectors.

Possible values: ENABLED, DISABLED Default value: DISABLED

CIInsight On enabling this option, the Citrix ADC will send the ContentInspection Insight records to the configured collectors.

Possible values: ENABLED, DISABLED Default value: DISABLED

videoAnalytics On enabling this option, the Citrix ADC will send the videoinsight records to the configured collectors.

Possible values: ENABLED, DISABLED Default value: DISABLED

distributionAlgorithm On enabling this option, the Citrix ADC will distribute records among the collectors. Else, all records will be sent to all the collectors.

Possible values: ENABLED, DISABLED Default value: DISABLED

TransactionLog Log ANOMALOUS or ALL transactions

Possible values: ALL, ANOMALOUS Default value: ALL

comment Any comments about this action. In the CLI, if including spaces between words, enclose the comment in quotation marks. (The quotation marks are not required in the configuration utility.)

Example

add appflow action appflow_action_1 -collectors col1 col2

appflow-collector

The following operations can be performed on "appflow-collector":

show| set| unset| rename| add| rm|

show appflow collector

Displays information about all configured AppFlow collectors, or about the specified collector.

Synopsis

show appflow collector

Arguments

name Name of the collector about which to display information.

Output

IPAddress IPv4 address of the collector.

port Port on which the collector listens.

netProfile Netprofile to associate with the collector. The IP address defined in the profile is used as the source IP address for AppFlow traffic for this collector. If you do not set this parameter, the Citrix ADC IP (NSIP) address is used as the source IP address.

Transport Type of collector: either logstream or ipfix or rest.

state Appflow collector state.

devno count stateflag

Example

show appflow collector collector1

set appflow collector

Sets an AppFlow collector. A collector receives the flow records generated by the Citrix ADC.

Synopsis

set appflow collector <name>

Arguments

name Name for the collector. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Only four collectors can be configured.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow collector" or 'my appflow collector').

IPAddress IPv4 address of the collector.

port Port on which the collector listens.

netProfile Netprofile to associate with the collector. The IP address defined in the profile is used as the source IP address for AppFlow traffic for this collector. If you do not set this parameter, the Citrix ADC IP (NSIP) address is used as the source IP address.

Example

set appflow collector collector1 -IPAddress 192.168.1.40 -port 2055

unset appflow collector

Use this command to remove appflow collector settings.Refer to the set appflow collector command for meanings of the arguments.

Synopsis

unset appflow collector <name>

rename appflow collector

Renames an AppFlow collector.

Synopsis

rename appflow collector <name>@ <newName>@

Arguments

name Existing name of the collector.

newName New name for the collector. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at(@), equals (=), and hyphen (-) characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow coll" or 'my appflow coll').

Example

rename appflow collector old_name new_name

add appflow collector

Adds a new AppFlow collector. A collector receives the flow records generated by the Citrix ADC. You can add only four AppFlow collectors to the Citrix ADC.

Synopsis

add appflow collector <name> -IPAddress <ip_addr>

Arguments

name Name for the collector. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Only four collectors can be configured.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow collector" or 'my appflow collector').

IPAddress IPv4 address of the collector.

port Port on which the collector listens.

netProfile Netprofile to associate with the collector. The IP address defined in the profile is used as the source IP address for AppFlow traffic for this collector. If you do not set this parameter, the Citrix ADC IP (NSIP) address is used as the source IP address.

Transport Type of collector: either logstream or ipfix or rest.

Possible values: ipfix, logstream, rest Default value: ipfix,

Example

add appflow collector collector1 -IPAddress 192.168.1.40 -port 2055

rm appflow collector

Removes an AppFlow collector. You cannot remove a collector if it is associated with an AppFlow action.

Synopsis

rm appflow collector <name>

Arguments

name Name of the collector to remove.

Example

rm appflow collector collector1

Appflow

The entities on which you can perform NetScaler CLI operations:

- appflow-action
- appflow
- appflow-collector
- appflow-global
- appflow-param
- appflow-policy
- appflow-policylabel

appflow-global

The following operations can be performed on "appflow-global":

show| unbind| bind|

show appflow global

Displays the AppFlow global bind points and the number of policies bound to each global bind point, or more detailed information about the specified bind point.

Synopsis

show appflow global

Arguments

type Global bind point for which to show detailed information about the policies bound to the bind point.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, OVERRIDE, DEFAULT, OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, MSSQL_REQ_OVERRIDE,

MSSQL_REQ_DEFAULT, MYSQL_REQ_OVERRIDE, MYSQL_REQ_DEFAULT, ICA_REQ_OVERRIDE, ICA_REQ_DEFAULT, ORACLE_REQ_OVERRIDE, ORACLE_REQ_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT

Output

stateflag policyName Name of the AppFlow policy.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke Invoke policies bound to a virtual server or a user-defined policy label. After the invoked policies are evaluated, the flow returns to the policy with the next priority.

labelType Type of policy label to invoke. Specify vserver for a policy label associated with a virtual server, or policylabel for a user-defined policy label.

labelName Name of the label to invoke if the current policy evaluates to TRUE.

numpol The number of policies bound to the bindpoint.

flowType Flow type of the bound AppFlow policy.

flags globalBindType devno count

Example

show appflow global

unbind appflow global

Unbinds entities from an AppFlow global bind point.

Synopsis

unbind appflow global (<policyName>)

Arguments

policyName Name of the policy to be unbound.

type Bind point from which to unbind the policy.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, OVERRIDE, DEFAULT, OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, MSSQL_REQ_OVERRIDE, MSSQL_REQ_DEFAULT, MYSQL_REQ_OVERRIDE, MYSQL_REQ_DEFAULT, ICA_REQ_OVERRIDE, ICA_REQ_DEFAULT, ORACLE_REQ_OVERRIDE, ORACLE_REQ_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT

priority Priority of the NOPOLICY to be unbound. Applicable only if a NOPOLICY has been bound to the bind point. Minimum value: 1 Maximum value: 2147483647

Example

unbind appflow global pol9

bind appflow global

Binds the AppFlow policy to one of the two global lists of AppFlow policies. A policy becomes active only after it is bound.

Synopsis

bind appflow global <policyName> <priority>

Arguments

policyName Name of the AppFlow policy to be bound.

priority Integer specifying the priority of the policy. The lower the number, the higher the priority. By default, policies in the list are evaluated in the order of their priority numbers. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the priority of the next policy, within the policy list, to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher numbered priority.
- END - Stop evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy list. If the final goto in the invoked policy list has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy list performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, it's evaluation result determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, that policy is evaluated next.

- If the expression evaluates to the priority of the current policy, the policy with the next higher priority number is evaluated next.
- If the expression evaluates to a priority number that is numerically higher than the highest priority number, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

type The bind point to which to bind the policy.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, OVERRIDE, DEFAULT, OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, MSSQL_REQ_OVERRIDE, MSSQL_REQ_DEFAULT, MYSQL_REQ_OVERRIDE, MYSQL_REQ_DEFAULT, ICA_REQ_OVERRIDE, ICA_REQ_DEFAULT, ORACLE_REQ_OVERRIDE, ORACLE_REQ_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT

invoke Invoke policies bound to a virtual server or a user-defined policy label. After the invoked policies are evaluated, the flow returns to the policy with the next priority.

labelType Type of policy label to invoke. Specify vserver for a policy label associated with a virtual server, or policylabel for a user-defined policy label.

Possible values: vserver, policylabel

labelName Name of the label to invoke if the current policy evaluates to TRUE.

Example

i)bind appflow global pol9 9 ii)bind appflow global pol9 9 120 iii)bind appflow global pol9 9 "HTTP.REQ.HEADER(\\"qh3\\").TYPECAST_NUM_T(DECIMAL)"

appflow-param

The following operations can be performed on "appflow-param":

show| set| unset|

show appflow param

Displays AppFlow parameters.

Synopsis

show appflow param

Arguments

Output

templateRefresh Refresh interval, in seconds, at which to export the template data. Because data transmission is in UDP, the templates must be resent at regular intervals.

appnameRefresh Interval, in seconds, at which to send Appnames to the configured collectors. Appname refers to the name of an entity (virtual server, service, or service group) in the Citrix ADC.

flowRecordInterval Interval, in seconds, at which to send flow records to the configured collectors.

SecurityInsightRecordInterval Interval, in seconds, at which to send security insight flow records to the configured collectors.

udpPmtu MTU, in bytes, for IPFIX UDP packets.

httpUrl State of AppFlow HTTP URL logging.

AAAUserName State of AppFlow AAA User logging.

httpCookie State of AppFlow HTTP cookie logging.

httpReferer State of AppFlow HTTP referer logging.

httpMethod State of AppFlow HTTP method logging.

httpHost State of AppFlow HTTP host logging.

httpUserAgent State of AppFlow HTTP user-agent logging.

clientTrafficOnly Generate AppFlow records for only the traffic from the client.

httpContentType State of AppFlow HTTP Content-Type header logging

httpAuthorization State of AppFlow HTTP Authorization header logging

httpVia State of AppFlow HTTP Via header logging

httpXForwardedFor State of AppFlow HTTP X-Forwarded-For header logging

httpLocation State of AppFlow HTTP Location header logging

httpSetCookie State of AppFlow HTTP Setcookie header logging

httpSetCookie2 State of AppFlow HTTP Setcookie2 header logging

connectionChaining State of connection-chaining feature

httpDomain State of AppFlow HTTP Domain name logging

skipCacheRedirectionHttpTransaction Skip Cache http transaction. This HTTP transaction is specific to Cache Redirection module. In Case of Cache Miss there will be another HTTP transaction initiated by the cache server.

identifierName State of AppFlow Stream Identifier Name logging

identifierSessionName State of AppFlow Stream Identifier Session Name logging

observationDomainId An observation domain groups a set of Citrix ADCs based on deployment: cluster, HA etc. A unique Observation Domain ID is required to be assigned to each such group.

observationPointId An observation point ID is identifier for the NetScaler from which appflow records are being exported. By default, the NetScaler IP is the observation point ID.

observationDomainName Name of the Observation Domain defined by the observation domain ID.

builtin Flag to determine if the appflow param is built-in or not

feature The feature to be checked while applying this config

SecurityInsightTraffic State of Security Insight traffic exporting

subscriberAwareness Enable this option for logging end user MSISDN in L4/L7 appflow records

subscriberIdObfuscation Enable this option for obfuscating MSISDN in L4/L7 appflow records

subscriberIdObfuscationAlgo Algorithm(MD5 or SHA256) to be used for obfuscating MSISDN

gxSessionReporting Enable this option for Gx session reporting

cacheInsight Flag to determine whether cache records need to be exported or not. If this flag is true and IC is enabled, cache records are exported instead of L7 HTTP records

videoInsight Enable/disable the feature individually on appflow action.

httpQueryWithUrl Include the HTTP query segment along with the URL that the Citrix ADC received from the client.

tcpBurstReporting TCP burst reporting enable/disable knob.

tcpBurstReportingThreshold TCP burst reporting threshold.

urlCategory Include the URL category record.

lsnLogging On enabling this option, the Citrix ADC will send the Large Scale Nat(LSN) records to the configured collectors.

cqaReporting TCP CQA reporting enable/disable knob.

emailAddress Enable AppFlow user email-id logging.

usageRecordInterval On enabling this option, the NGS will send bandwidth usage record to configured collectors.

webSaasAppUsageReporting On enabling this option, NGS will send data used by Web/saas app at the end of every HTTP transaction to configured collectors.

metrics Enable Citrix ADC Stats to be sent to the Telemetry Agent

events Enable Events to be sent to the Telemetry Agent

auditlogs Enable Auditlogs to be sent to the Telemetry Agent

distributedTracing Enable generation of the distributed tracing templates in the Appflow records

distTracingSamplingRate Sampling rate for Distributed Tracing

tcpAttackCounterInterval Interval, in seconds, at which to send tcp attack counters to the configured collectors. If 0 is configured, the record is not sent.

logstreamOverNSIP To use the Citrix ADC IP to send Logstream records instead of the SNIP

analyticsAuthToken Authentication token to be set by the agent.

TimeseriesOverNSIP To use the Citrix ADC IP to send Time series data such as metrics and events, instead of the SNIP

set appflow param

Configures AppFlow parameters.

Synopsis

set appflow param [-subscriberIdObfuscation (ENABLED | DISABLED)]

Arguments

templateRefresh Refresh interval, in seconds, at which to export the template data. Because data transmission is in UDP, the templates must be resent at regular intervals. Default value: 600 Minimum value: 60 Maximum value: 3600

appnameRefresh Interval, in seconds, at which to send Appnames to the configured collectors. Appname refers to the name of an entity (virtual server, service, or service group) in the Citrix ADC. Default value: 600 Minimum value: 60 Maximum value: 3600

flowRecordInterval Interval, in seconds, at which to send flow records to the configured collectors. Default value: 60 Minimum value: 60 Maximum value: 3600

SecurityInsightRecordInterval Interval, in seconds, at which to send security insight flow records to the configured collectors. Default value: 600 Minimum value: 60 Maximum value: 3600

udpPmtu MTU, in bytes, for IPFIX UDP packets. Default value: 1472 Minimum value: 128 Maximum value: 1472

httpUrl Include the http URL that the Citrix ADC received from the client.

Possible values: ENABLED, DISABLED Default value: DISABLED

AAAUserName Enable AppFlow AAA Username logging.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpCookie Include the cookie that was in the HTTP request the appliance received from the client.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpReferer Include the web page that was last visited by the client.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpMethod Include the method that was specified in the HTTP request that the appliance received from the client.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpHost Include the host identified in the HTTP request that the appliance received from the client.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpUserAgent Include the client application through which the HTTP request was received by the Citrix ADC.

Possible values: ENABLED, DISABLED Default value: DISABLED

clientTrafficOnly Generate AppFlow records for only the traffic from the client.

Possible values: YES, NO Default value: NO

httpContentType Include the HTTP Content-Type header sent from the server to the client to determine the type of the content sent.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpAuthorization Include the HTTP Authorization header information.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpVia Include the httpVia header which contains the IP address of proxy server through which the client accessed the server.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpXForwardedFor Include the httpXForwardedFor header, which contains the original IP Address of the client using a proxy server to access the server.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpLocation Include the HTTP location headers returned from the HTTP responses.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpSetCookie Include the Set-cookie header sent from the server to the client in response to a HTTP request.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpSetCookie2 Include the Set-cookie header sent from the server to the client in response to a HTTP request.

Possible values: ENABLED, DISABLED Default value: DISABLED

connectionChaining Enable connection chaining so that the client server flows of a connection are linked. Also the connection chain ID is propagated across Citrix ADCs, so that in a multi-hop environment the flows belonging to the same logical connection are linked. This id is also logged as part of appflow record

Possible values: ENABLED, DISABLED Default value: DISABLED

httpDomain Include the http domain request to be exported.

Possible values: ENABLED, DISABLED Default value: DISABLED

skipCacheRedirectionHttpTransaction Skip Cache http transaction. This HTTP transaction is specific to Cache Redirection module. In Case of Cache Miss there will be another HTTP transaction initiated by the cache server.

Possible values: ENABLED, DISABLED Default value: DISABLED

identifierName Include the stream identifier name to be exported.

Possible values: ENABLED, DISABLED Default value: DISABLED

identifierSessionName Include the stream identifier session name to be exported.

Possible values: ENABLED, DISABLED Default value: DISABLED

observationDomainId An observation domain groups a set of Citrix ADCs based on deployment: cluster, HA etc. A unique Observation Domain ID is required to be assigned to each such group. Default value: 0 Minimum value: 1000

observationDomainName Name of the Observation Domain defined by the observation domain ID.

subscriberAwareness Enable this option for logging end user MSISDN in L4/L7 appflow records

Possible values: ENABLED, DISABLED Default value: DISABLED

subscriberIdObfuscation Enable this option for obfuscating MSISDN in L4/L7 appflow records

Possible values: ENABLED, DISABLED Default value: DISABLED

subscriberIdObfuscationAlgo Algorithm(MD5 or SHA256) to be used for obfuscating MSISDN

Possible values: MD5, SHA256 Default value: MD5

gxSessionReporting Enable this option for Gx session reporting

Possible values: ENABLED, DISABLED Default value: DISABLED

SecurityInsightTraffic Enable/disable the feature individually on appflow action.

Possible values: ENABLED, DISABLED Default value: DISABLED

cacheInsight Flag to determine whether cache records need to be exported or not. If this flag is true and IC is enabled, cache records are exported instead of L7 HTTP records

Possible values: ENABLED, DISABLED Default value: DISABLED

videoInsight Enable/disable the feature individually on appflow action.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpQueryWithUrl Include the HTTP query segment along with the URL that the Citrix ADC received from the client.

Possible values: ENABLED, DISABLED Default value: DISABLED

urlCategory Include the URL category record.

Possible values: ENABLED, DISABLED Default value: DISABLED

lsnLogging On enabling this option, the Citrix ADC will send the Large Scale Nat(LSN) records to the configured collectors.

Possible values: ENABLED, DISABLED Default value: DISABLED

cqaReporting TCP CQA reporting enable/disable knob.

Possible values: ENABLED, DISABLED Default value: DISABLED

emailAddress Enable AppFlow user email-id logging.

Possible values: ENABLED, DISABLED Default value: DISABLED

usageRecordInterval On enabling this option, the NGS will send bandwidth usage record to configured collectors. Default value: 0 Minimum value: 0 Maximum value: 7200

webSaasAppUsageReporting On enabling this option, NGS will send data used by Web/saas app at the end of every HTTP transaction to configured collectors.

Possible values: ENABLED, DISABLED Default value: DISABLED

metrics Enable Citrix ADC Stats to be sent to the Telemetry Agent

Possible values: ENABLED, DISABLED Default value: DISABLED

events Enable Events to be sent to the Telemetry Agent

Possible values: ENABLED, DISABLED Default value: DISABLED

auditlogs Enable Auditlogs to be sent to the Telemetry Agent

Possible values: ENABLED, DISABLED Default value: DISABLED

observationPointId An observation point ID is identifier for the NetScaler from which appflow records are being exported. By default, the NetScaler IP is the observation point ID. Minimum value: 1

distributedTracing Enable generation of the distributed tracing templates in the Appflow records

Possible values: ENABLED, DISABLED Default value: DISABLED

distTracingSamplingRate Sampling rate for Distributed Tracing Default value: 0 Minimum value: 0 Maximum value: 100

tcpAttackCounterInterval Interval, in seconds, at which to send tcp attack counters to the configured collectors. If 0 is configured, the record is not sent. Default value: 0 Maximum value: 3600

logstreamOverNSIP To use the Citrix ADC IP to send Logstream records instead of the SNIP

Possible values: ENABLED, DISABLED Default value: DISABLED

analyticsAuthToken Authentication token to be set by the agent. Maximum value: 256

TimeseriesOverNSIP To use the Citrix ADC IP to send Time series data such as metrics and events, instead of the SNIP

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set appflow param -templateRefresh 240

unset appflow param

Use this command to remove appflow param settings.Refer to the set appflow param command for meanings of the arguments.

Synopsis

unset appflow param

appflow-policy

The following operations can be performed on "appflow-policy":

unset| show| set| rm| add| rename|

unset appflow policy

Use this command to remove appflow policy settings.Refer to the set appflow policy command for meanings of the arguments.

Synopsis

unset appflow policy <name>

show appflow policy

Displays information about all configured AppFlow policies, or detailed information about the specified policy.

Synopsis

show appflow policy

Arguments

name Name of the policy about which to display detailed information.

Output

stateflag rule Expression to be used by AppFlow policy.

action AppFlow action associated with the policy.

undefAction AppFlow action associated with the policy on undefined evaluation result.

hits Number of hits.

undefHits Number of policy UNDEF hits.

activePolicy Indicates whether policy is bound or not.

boundTo Location where policy is bound.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

description Description of the policy

comment Any comments about this policy.

bindPolicyType vserverType type builtin Flag to determine if policy is built-in or not

feature The feature to be checked while applying this config

devno count

Example

show appflow policy

set appflow policy

Modifies the rule and/or action for an existing AppFlow policy. The rule for flow type can be changed only if the associated action is of NEUTRAL flow type.

Synopsis

set appflow policy <name>

Arguments

name Name of the policy to modify.

rule Expression or other value against which the traffic is evaluated. Must be a Boolean expression.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the action to be associated with this policy.

undefAction Name of the appflow action to be associated with this policy when an undef event occurs.

comment Any comments about this policy.

Example

set appflow policy appflow_policy -rule "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh2\\")"

rm appflow policy

Removes an AppFlow policy. (Cannot remove a policy that is bound to a policy label.)

Synopsis

rm appflow policy <name>

Arguments

name Name of the policy to be removed.

Example

rm appflow policy appflow_policy_1

add appflow policy

Adds an Appflow policy. The policy specifies the rule based on which the traffic is evaluated, and the action to be taken if the rule returns "TRUE".

Synopsis

add appflow policy <name> <rule> <action>

Arguments

name Name for the policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow policy" or 'my appflow policy').

rule Expression or other value against which the traffic is evaluated. Must be a Boolean expression.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the action to be associated with this policy.

undefAction Name of the appflow action to be associated with this policy when an undef event occurs.

comment Any comments about this policy.

Example

add appflow policy appflow_pol "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh3\\")" appflow_act

rename appflow policy

Renames an AppFlow policy.

Synopsis

rename appflow policy <name>@ <newName>@

Arguments

name Existing name of the policy.

newName New name for the policy. Must begin with an ASCII alphabetic or underscore (_)character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow policy" or 'my appflow policy').

Example

rename appflow policy old_name new_name

appflow-policylabel

The following operations can be performed on "appflow-policylabel":

unbind| rm| add| rename| show| bind|

unbind appflow policylabel

Unbinds an AppFlow policy from an AppFlow policy label.

Synopsis

unbind appflow policylabel <labelName> <policyName>

Arguments

labelName Name of the policy label from which to unbind a policy.

policyName Name of the policy to unbind.

priority Priority of the NOPOLICY to be unbound. Applicable only if a NOPOLICY has been bound to the policy label. Minimum value: 1 Maximum value: 2147483647

Example

unbind appflow policylabel appflow_pol_label appflow_pol

rm appflow policylabel

Removes an AppFlow policy label.

Synopsis

rm appflow policylabel <labelName>

Arguments

labelName Name of the policy label to be removed.

Example

rm appflow policylabel appflow_pol_label

add appflow policylabel

Creates a user-defined AppFlow policy label. You can bind AppFlow policies to the AppFlow policy label.

Synopsis

add appflow policylabel <labelName>

Arguments

labelName Name of the AppFlow policy label. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow policylabel" or 'my appflow policylabel').

policylabeltype Type of traffic evaluated by the policies bound to the policy label.

Possible values: HTTP, OTHERTCP, HTTP_QUIC Default value: HTTP

Example

add appflow policylabel appflow_pol_label

rename appflow policylabel

Renames an AppFlow policy label.

Synopsis

rename appflow policylabel <labelName>@ <newName>@

Arguments

labelName Existing name of the policylabel.

newName New name for the policy label. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

```
The following requirement applies only to the Citrix ADC CLI:
```

If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow policylabel" or 'my appflow policylabel')

Example

rename appflow policylabel old_name new_name

show appflow policylabel

Displays information about all AppFlow policy labels, or detailed information about the specified policy label.

Synopsis

show appflow policylabel

Arguments

labelName Name of the policy label about which to display detailed information.

Output

stateflag policylabeltype Type of traffic evaluated by the policies bound to the policy label.

numpol Number of polices bound to the policy label.

hits Number of times the policy label was invoked.

policyName Name of the AppFlow policy.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke Invoke policies bound to a virtual server or a user-defined policy label. After the invoked policies are evaluated, the flow returns to the policy with the next priority.

labelType Type of policy label to be invoked.

labelName Name of the label to invoke if the current policy evaluates to TRUE.

flowType Flowtype of the bound AppFlow policy.

description Description of the policylabel

flags devno count

Example

i)show appflow policylabel appflow_pol_label ii)show appflow policylabel

bind appflow policylabel

Binds an AppFlow policy to an AppFlow policy label.

Synopsis

bind appflow policylabel <labelName> -policyName <string> -priority <positive_integer>

Arguments

labelName Name of the policy label to which to bind the policy.

policyName Name of the policy to bind to the policy label.

priority Priority assigned to the policy. The lower the number, the higher the priority. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the priority of the next policy, within the policy label, to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher numbered priority.
- END - Stop evaluation.

- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, it's evaluation result determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, that policy is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher priority number is evaluated next.
- If the expression evaluates to a priority number that is numerically higher than the highest priority number, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

invoke Invoke policies bound to a virtual server or a user-defined policy label. After the invoked policies are evaluated, the flow returns to the policy with the next priority.

labelType Type of policy label to be invoked.

Possible values: vserver, policylabel

labelName Name of the label to invoke if the current policy evaluates to TRUE.

Example

bind appflow policylabel appflow_pol_label -policyName appflow_pol -priority 1

appflow

The following operations can be performed on "appflow":

stat appflow

Display AppFlow statistics.

Synopsis

stat appflow

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

AppFlow octets transmitted (aflwOcts) The total number of AppFlow (IPFIX) octets that the Citrix ADC has transmitted.

AppFlow flows transmitted (aflwFlws) The total number of AppFlow (IPFIX) flows that the Citrix ADC has transmitted.

AppFlow messages transmitted (aflwMsgs) The total number of AppFlow (IPFIX) messages that the Citrix ADC has transmitted.

Octets ignored for AppFlow (aflwIgnOct) The total number of octets that the Citrix ADC has ignored for AppFlow (IPFIX).

Packets ignored for AppFlow (aflwIgnPkts) The total number of packets that the Citrix ADC has ignored for AppFlow (IPFIX).

AppFlow octets not transmitted (aflwNoTxOcts) The total number of AppFlow (IPFIX) octets that the Citrix ADC has not transmitted.

AppFlow flows not transmitted (aflwNoTxFlows) The total number of AppFlow (IPFIX) flows that the Citrix ADC has not transmitted.

AppFlow packets not transmitted (aflwNoTxPkts) The total number of AppFlow (IPFIX) packets that the Citrix ADC has not transmitted.

appfw

appfw-JSONContentType

The following operations can be performed on "appfw-JSONContentType":

show| rm| add|

show appfw JSONContentType

Display all JSON content types.

Synopsis

show appfw JSONContentType

Arguments

JSONContenttypevalue Content type to be classified as JSON

Output

isRegex Is json content type a regular expression?

builtin Flag to determine if jsoncontenttype is built-in or not

feature The feature to be checked while applying this config

devno count stateflag

rm appfw JSONContentType

Remove JSON content type.

Synopsis

rm appfw JSONContentType <JSONContenttypevalue>

Arguments

JSONContenttypevalue Content type to be classified as JSON

add appfw JSONContentType

Add JSON content type. This will classify a request/response with the specified content type as JSON

Synopsis

add appfw JSONContentType <JSONContenttypevalue>

Arguments

JSONContenttypevalue Content type to be classified as JSON

isRegex Is json content type a regular expression?

Possible values: REGEX, NOTREGEX Default value: NOTREGEX

appfw-XMLContentType

The following operations can be performed on "appfw-XMLContentType":

add| rm| show|

add appfw XMLContentType

Add XML content type. This will classify a request/response with the specified content type as XML

Synopsis

add appfw XMLContentType <XMLContenttypevalue>

Arguments

XMLContenttypevalue Content type to be classified as XML

isRegex Is field name a regular expression?

Possible values: REGEX, NOTREGEX Default value: NOTREGEX

rm appfw XMLContentType

Remove XML content type.

Synopsis

rm appfw XMLContentType <XMLContenttypevalue>

Arguments

XMLContenttypevalue Content type to be classified as XML

show appfw XMLContentType

Display all xml content types.

Synopsis

show appfw XMLContentType

Arguments

XMLContenttypevalue Content type to be classified as XML

Output

isRegex Is field name a regular expression?

builtin Flag to determine if xmlcontenttype is built-in or not

feature The feature to be checked while applying this config

devno count stateflag

appfw-archive

The following operations can be performed on "appfw-archive":

export| show| rm| import|

export appfw archive

Exports the archive file to the specified location

Synopsis

export appfw archive <name> <target>

Arguments

name Name of tar archive

target Path to the file to be exported

Related Commands

- restore appfw profile

show appfw archive

Synopsis

show appfw archive

Output

response

Example

show appfw archive

rm appfw archive

Removes the archive created by archive command.

Synopsis

rm appfw archive <name>

Arguments

name Indicates name of the archive to be removed.

Example

rm appfw archive <name>

import appfw archive

Imports the archive file from specified location

Synopsis

import appfw archive <src> <name>

Arguments

src Indicates the source of the tar archive file as a URL of the form

```
&lt;protocol&gt;://&lt;host&gt;[:&lt;port&gt;][/&lt;path&gt;]
```

<protocol> is http or https. <host> is the DNS name or IP address of the http or https server. <port> is the port number of the server. If omitted, the default port for http or https will be used. <path> is the path of the file on the server.

Import will fail if an https server requires client certificate authentication.

name Indicates name of archive

comment Comments associated with this archive.

Related Commands

- restore appfw profile

Appfw

The entities on which you can perform NetScaler CLI operations:

- appfw-JSONContentType
- appfw-XMLContentType
- appfw
- appfw-archive
- appfw-confidField
- appfw-customSettings
- appfw-fieldType
- appfw-gRPCContentType
- appfw-gRpcWebJSONContentType
- appfw-gRpcWebTextContentType
- appfw-global
- appfw-htmlerrorpage
- appfw-jsonerrorpage
- appfw-learningdata
- appfw-learningsettings
- appfw-multipartFormContentType
- appfw-policy
- appfw-policylabel

- appfw-profile
- appfw-protofile
- appfw-settings
- appfw-signatures
- appfw-stats
- appfw-transactionRecords
- appfw-urlEncodedFormContentType
- appfw-wsdl
- appfw-xmlerrorpage
- appfw-xmlschema

appfw-confidField

The following operations can be performed on "appfw-confidField":

rm| add| show| set| unset|

rm appfw confidField

Removes a confidential field designation.

Synopsis

rm appfw confidField <fieldName> <url>

Arguments

fieldName Name of the web form field.

url URL of the web page that contains the web form in which the field appears.

add appfw confidField

Defines the specified web form field as confidential. Form fields designated as confidential have the information that is provided in those fields x'd out in the audit logs.

Synopsis

add appfw confidField <fieldName> <url>

Arguments

fieldName Name of the form field to designate as confidential.

url URL of the web page that contains the web form.

isRegex Method of specifying the form field name. Available settings function as follows:

- REGEX. Form field is a regular expression.
- NOTREGEX. Form field is a literal string.

Possible values: REGEX, NOTREGEX Default value: NOTREGEX

comment Any comments to preserve information about the form field designation.

state Enable or disable the confidential field designation.

Possible values: ENABLED, DISABLED Default value: ENABLED

show appfw confidField

Displays the current settings for the specified application firewall confidential field designation. If no confidential field designation is specified, displays a list of all application firewall confidential field designations on the Citrix ADC.

Synopsis

show appfw confidField

Arguments

fieldName Name of the web form field.

url URL of the web page that contains the web form with the form field.

Output

isRegex Method of specifying the form field name. Available settings function as follows:

- REGEX. Form field is a regular expression.
- NOTREGEX. Form field is a literal string.

comment Any comments to preserve information about the form field designation.

state Enable or disable the confidential field designation.

devno count stateflag

set appfw confidField

Modifies the specified parameters of a confidential field setting. Form fields designated as confidential have the information that is provided in those fields x'd out in the audit logs.

Synopsis

set appfw confidField <fieldName> <url>

Arguments

fieldName Name of the field to modify.

url URL of the web page that contains the web form.

comment Any comments to preserve information about the form field designation.

isRegex Method of specifying the form field name. Available settings function as follows:

- REGEX. Form field is a regular expression.
- NOTREGEX. Form field is a literal string.

Possible values: REGEX, NOTREGEX Default value: NOTREGEX

state Enable or disable the confidential field designation.

Possible values: ENABLED, DISABLED Default value: ENABLED

unset appfw confidField

Use this command to remove appfw confidField settings.Refer to the set appfw confidField command for meanings of the arguments.

Synopsis

unset appfw confidField <fieldName> <url>

appfw-customSettings

The following operations can be performed on "appfw-customSettings":

rm| update| import| export| show|

rm appfw customSettings

Removes the object imported by import customsettings. NOTE: This command is deprecated.Changed CLI commands for Appfw "customSettings" to "signatures"

Synopsis

Arguments

name Indicates name of custom-settings object.

Example

rm customsettings <name>

update appfw customSettings

Updates the Application Firewall Custom Settings XML configuration to the Citrix ADC Box with the given object name NOTE: This command is deprecated.Changed CLI commands for Appfw "customSettings" to "signatures"

Synopsis

Arguments

name Indicates name of the custom-settings object to update.

Example

update customsettings my-settings

import appfw customSettings

Downloads the Application Firewall Custom Settings XML configuration to the Citrix ADC Box with the given object name NOTE: This command is deprecated.Changed CLI commands for Appfw "customSettings" to "signatures"

Synopsis

Arguments

src Indicates the source of the custom settings file as a URL of the form

```
&lt;protocol&gt;://&lt;host&gt;[:&lt;port&gt;][/&lt;path&gt;]
```

is http or https.is the DNS name or IP address of the http or https server.is the port number of the server. If omitted, the default port for http or https will be used.is the path of the file on the server.

Import will fail if an https server requires client certificate authentication.

name Indicates name of custom-settings object.

comment Comments.

xslt XSLT file URL.

merge Merges the existing Signature with new signature rules

preservedefactions preserves the def actions on a signature rule in signature object

overwrite Overwrites the existing file

sha1 File path for sha1 file to validate signature file

Example

import customsettings http://www.example.com/ns/customsettings.xml my-settings

export appfw customSettings

NOTE: This command is deprecated.Changed CLI commands for Appfw "customSettings" to "signatures"

Synopsis

Arguments

name target

show appfw customSettings

Displays the object imported by import customsettings. NOTE: This command is deprecated.Changed CLI commands for Appfw "customSettings" to "signatures"

Synopsis

Arguments

name

Output

response

Example

show appfw customsettings

appfw-fieldType

The following operations can be performed on "appfw-fieldType":

add| show| set| rm|

add appfw fieldType

Adds a field type to the list of field types used by the field format security check. A field type is a regular expression defining the type of data that can appear in a web form field. The Learning engine also uses the field types list to generate appropriate field type assignments for the field formats check.

Synopsis

add appfw fieldType <name> <regex> <priority>

Arguments

name Name for the field type. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the field type is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my field type" or 'my field type').

regex PCRE - format regular expression defining the characters and length allowed for this field type.

priority Positive integer specifying the priority of the field type. A lower number specifies a higher priority. Field types are checked in the order of their priority numbers. Minimum value: 0 Maximum value: 64000

comment Comment describing the type of field that this field type is intended to match.

show appfw fieldType

Displays the regular expression that defines the specified field type and its priority. If no field type is specified, displays all form field types currently configured on the Citrix ADC.

Synopsis

show appfw fieldType

Arguments

name Name of the field type.

noCharMaps will not show internal field types added as part of FieldFormat learn rules deployment

Output

regex PCRE - format regular expression defining the characters and length allowed for this field type.

priority Positive integer specifying the priority of the field type. A lower number specifies a higher priority. Field types are checked in the order of their priority numbers.

comment Comment describing the type of field that this field type is intended to match.

builtin Flag to determine if fieldtype is built-in or not

feature The feature to be checked while applying this config

devno count stateflag

set appfw fieldType

Modifies the properties of the specified application firewall field type.

Synopsis

set appfw fieldType <name> <regex> <priority>

Arguments

name Name for the field type. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the field type is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my field type" or 'my field type').

regex PCRE - format regular expression defining the characters and length allowed for this field type.

priority Positive integer specifying the priority of the field type. A lower number specifies a higher priority. Field types are checked in the order of their priority numbers. Minimum value: 0 Maximum value: 64000

comment Comment describing the type of field that this field type is intended to match.

rm appfw fieldType

Removes an application firewall field type.

Synopsis

rm appfw fieldType <name>

Arguments

name Name of the field type.

appfw-gRPCContentType

The following operations can be performed on "appfw-gRPCContentType":

rm| show| add|

rm appfw gRPCContentType

Remove gRPC content type.

Synopsis

rm appfw gRPCContentType <gRPCContenttypevalue>

Arguments

gRPCContenttypevalue Content type to be classified as gRPC

show appfw gRPCContentType

Display all gRPC content types.

Synopsis

show appfw gRPCContentType

Arguments

gRPCContenttypevalue Content type to be classified as gRPC

Output

isRegex Is gRPC content type a regular expression?

builtin Flag to determine if gRPC content type is built-in or not

feature The feature to be checked while applying this config

devno count stateflag

add appfw gRPCContentType

Add gRPC content type. This will classify a request/response with the specified content type as gRPC

Synopsis

add appfw gRPCContentType <gRPCContenttypevalue>

Arguments

gRPCContenttypevalue Content type to be classified as gRPC

isRegex Is gRPC content type a regular expression?

Possible values: REGEX, NOTREGEX Default value: NOTREGEX

appfw-gRpcWebJSONContentType

The following operations can be performed on "appfw-gRpcWebJSONContentType":

add| rm| show|

add appfw gRpcWebJSONContentType

Add gRPC-web-json content type. This will classify a request/response with the specified content type as gRPC-web-json

Synopsis

add appfw gRpcWebJSONContentType <gRPCWebJSONContenttypevalue>

Arguments

gRPCWebJSONContenttypevalue Content type to be classified as gRPC-web-json

isRegex Is gRPC-web-json content type a regular expression?

Possible values: REGEX, NOTREGEX Default value: NOTREGEX

rm appfw gRpcWebJSONContentType

Remove grpc-web-json content type.

Synopsis

rm appfw gRpcWebJSONContentType <gRPCWebJSONContenttypevalue>

Arguments

gRPCWebJSONContenttypevalue Content type to be classified as gRPC-web-json

show appfw gRpcWebJSONContentType

Display all grpc-web-json content types.

Synopsis

show appfw gRpcWebJSONContentType

Arguments

gRPCWebJSONContenttypevalue Content type to be classified as gRPC-web-json

Output

isRegex Is gRPC-web-json content type a regular expression?

devno count stateflag

appfw-gRpcWebTextContentType

The following operations can be performed on "appfw-gRpcWebTextContentType":

show| add| rm|

show appfw gRpcWebTextContentType

Display all grpc-web-text content types.

Synopsis

show appfw gRpcWebTextContentType

Arguments

gRPCWebTextContenttypevalue Content type to be classified as gRPC-web-text

Output

isRegex Is gRPC-web-text content type a regular expression?

devno count stateflag

add appfw gRpcWebTextContentType

Add gRPC-web-text content type. This will classify a request/response with the specified content type as gRPC-web-text

Synopsis

add appfw gRpcWebTextContentType <gRPCWebTextContenttypevalue>

Arguments

gRPCWebTextContenttypevalue Content type to be classified as gRPC-web-text

isRegex Is gRPC-web-text content type a regular expression?

Possible values: REGEX, NOTREGEX Default value: NOTREGEX

rm appfw gRpcWebTextContentType

Remove grpc-web-text content type.

Synopsis

rm appfw gRpcWebTextContentType <gRPCWebTextContenttypevalue>

Arguments

gRPCWebTextContenttypevalue Content type to be classified as gRPC-web-text

appfw-global

The following operations can be performed on "appfw-global":

unbind| show| bind|

unbind appfw global

Deactivates the specified application firewall policy. See the bind appfw policy command for descriptions of the parameters.

Synopsis

unbind appfw global <policyName>

Arguments

policyName Application Firewall policy name.

type The bindpoint from which the policy is to be unbound.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, NONE

priority Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

show appfw global

Displays a list of application firewall policies that are bound to the specified bind point. If no bind point is specified, displays a list of all application firewall policies

Synopsis

show appfw global

Arguments

type Bind point to which to policy is bound.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, NONE

Output

policyName Name of the policy.

priority The priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

state Enable or disable the binding to activate or deactivate the policy. This is applicable to classic policies only.

bindPolicyType The type of the policy.

policySubType stateflag stateflag

labelType Type of policy label invocation.

labelName Name of the policy label to invoke if the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is set to Policy Label.

flowType flowtype of the bound application firewall policy.

numpol The number of policies bound to the bindpoint.

flags policyType flag globalBindType devno count

bind appfw global

Activates an application firewall policy.

Synopsis

bind appfw global <policyName> <priority>

Arguments

policyName Name of the policy.

priority Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Must be unique within the group of policies that are bound to the global bind point. Policies

are evaluated in the order of their priority numbers. Minimum value: 0 Maximum value: 2147483647

state Enable or disable the binding to activate or deactivate the policy. This is applicable to classic policies only.

Possible values: ENABLED, DISABLED Default value: ENABLED

gotoPriorityExpression Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.
- The expression evaluates to a priority number that is smaller than the current policy's priority number.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

type Bind point to which to bind the policy. Can be used only with Citrix ADC default policies. Citrix ADC classic policies are not supported. Available settings function as follows:

- REQ_OVERRIDE. Request override. Binds the policy to the priority request queue.
- REQ_DEFAULT. Binds the policy to the default request queue.
- HTTPQUIC_REQ_OVERRIDE. Binds the policy to the HTTP_QUIC override request queue.
- HTTPQUIC_REQ_DEFAULT. Binds the policy to the HTTP_QUIC default request queue.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, NONE

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

labelType Type of policy label to invoke if the current policy evaluates to TRUE and the invoke parameter is set. Available settings function as follows:

- reqvserver. Invoke the unnamed policy label associated with the specified request virtual server.
- policylabel. Invoke the specified user-defined policy label.

Possible values: reqvserver, policylabel

labelName Name of the policy label to invoke if the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is set to Policy Label.

appfw-htmlerrorpage

The following operations can be performed on "appfw-htmlerrorpage":

rm| import| show| update|

rm appfw htmlerrorpage

Removes the specified HTML error object.

Synopsis

rm appfw htmlerrorpage <name>

Arguments

name Name of the XML error object to remove.

Example

rm htmlerrorpage <name>

import appfw htmlerrorpage

Imports the specified HTML error page to the Citrix ADC and assigns it the specified name.

Synopsis

import appfw htmlerrorpage <src> <name>

Arguments

src URL (protocol, host, path, and name) for the location at which to store the imported HTML error object. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

name Name to assign to the HTML error object on the Citrix ADC.

comment Any comments to preserve information about the HTML error object.

overwrite Overwrite any existing HTML error object of the same name.

Example

import htmlerrorpage http://www.example.com/errorpage.html my-html-error-page

show appfw htmlerrorpage

Displays the specified HTML error object. If no HTML error object is specified, lists all HTML error objects on the Citrix ADC.

Synopsis

show appfw htmlerrorpage

Arguments

name Name of the HTML error object.

Output

response src URL (protocol, host, path, and name) for the location at which to store the imported HTML error object. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

Example

show appfw htmlerrorpage

update appfw htmlerrorpage

Updates the specified HTML error object from the source.

Synopsis

update appfw htmlerrorpage <name>

Arguments

name Name of the HTML error page object to update.

Example

update htmlerrorpage my-html-error-page

appfw-jsonerrorpage

The following operations can be performed on "appfw-jsonerrorpage":

rm| show| update| import|

rm appfw jsonerrorpage

Removes the object imported by import jsonerrorpage.

Synopsis

rm appfw jsonerrorpage <name>

Arguments

name Indicates name of the imported json error page to be removed.

Example

rm jsonerrorpage <name>

show appfw jsonerrorpage

Displays the specified JSON error object. If no JSON error page object is specified, displays a list of all JSON error objects on the Citrix ADC.

Synopsis

show appfw jsonerrorpage

Arguments

name Name of the JSON error object.

Output

response JSON error object contents

src URL (protocol, host, path, and name) for the location at which to store the imported JSON error object. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

Example

show appfw jsonerrorpage

update appfw jsonerrorpage

Updates the specified JSON error object from the source.

Synopsis

update appfw jsonerrorpage <name>

Arguments

name Name of the JSON error object.

Example

update jsonerrorpage my-json-error-page

import appfw jsonerrorpage

Imports the specified JSON error page to the Citrix ADC and assigns it the specified name.

Synopsis

import appfw jsonerrorpage <src> <name>

Arguments

src URL (protocol, host, path, and name) for the location at which to store the imported JSON error object. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

name Name to assign to the JSON error object on the Citrix ADC.

comment Any comments to preserve information about the JSON error object.

overwrite Overwrite any existing JSON error object of the same name.

Example

import jsonerrorpage http://www.example.com/errorpage.json my-json-error-page

appfw-learningdata

The following operations can be performed on "appfw-learningdata":

reset| rm| show| export|

reset appfw learningdata

Remove all databases. Make transaction count zero

Synopsis

reset appfw learningdata

rm appfw learningdata

Removes unreviewed application firewall learning data for the specified application firewall profile.

Synopsis

rm appfw learningdata <profileName> (-startURL <expression> | -cookieConsistency <string> | (-fieldConsistency <string> <formActionURL>) | -contentType <string> | (-crossSiteScripting <string> <formActionURL>) | (-SQLInjection <string> <formActionURL>) | (-fieldFormat <string> <formActionURL>) | (-CSRFTag <expression> <CSRFFormOriginURL>) | (-CreditCardNumber <expression> <CreditCardNumberUrl>) | -XMLDoSCheck <expression> | -XMLWSICheck <expression> | -XMLAttachmentCheck <expression>)

Arguments

profileName Name of the profile.

startURL Start URL configuration.

cookieConsistency Cookie Name.

fieldConsistency Form field name.

formActionURL Form action URL.

contentType Content Type Name.

crossSiteScripting Cross-site scripting.

formActionURL Form action URL.

location Location of cross-site scripting exception - form field, header, cookie or url.

Possible values: FORMFIELD, HEADER, COOKIE, URL

valueType XSS value type. (Tag | Attribute | Pattern)

Possible values: Tag, Attribute, Pattern

valueExpression XSS value expressions consistituting expressions for Tag, Attribute or Pattern.

SQLInjection Form field name.

formActionURL Form action URL.

location Location of sql injection exception - form field, header or cookie.

Possible values: FORMFIELD, HEADER, COOKIE

valueType SQL value type. Keyword, SpecialString or Wildchar

Possible values: Keyword, SpecialString, Wildchar

valueExpression SQL value expressions consistituting expressions for Keyword, SpecialString or Wildchar.

fieldFormat Field format name.

formActionURL Form action URL.

CSRFTag CSRF Form Action URL

CSRFFormOriginURL CSRF Form Origin URL.

CreditCardNumber The object expression that is to be excluded from safe commerce check.

CreditCardNumberUrl The url for which the list of credit card numbers are needed to be bypassed from inspection

XMLDoSCheck XML Denial of Service check, one of MaxAttributes MaxAttributeNameLength MaxAttributeValueLength MaxElementNameLength MaxFileSize MinFileSize MaxCDATALength MaxElements MaxElementDepth MaxElementChildren NumDTDs NumProcessingInstructions NumExternalEntities MaxEntityExpansions MaxEntityExpansionDepth MaxNamespaces MaxNamespaceUriLength MaxSOAPArraySize MaxSOAPArrayRank

XMLWSICheck Web Services Interoperability Rule ID.

XMLAttachmentCheck XML Attachment Content-Type.

TotalXMLRequests Total XML requests.

show appfw learningdata

Displays the unreviewed application firewall learning data for the specified profile and security check.

Synopsis

show appfw learningdata <profileName> <securityCheck>

Arguments

profileName Name of the profile.

securityCheck Name of the security check.

Possible values: startURL, cookieConsistency, fieldConsistency, crossSiteScripting, SQLInjection, fieldFormat, CSRFtag, XMLDoSCheck, XMLWSICheck, XMLAttachmentCheck, TotalXMLRequests, creditCardNumber, ContentType

Output

url Learnt url

name Learnt field name

fieldType Learnt field type

fieldFormatMinLength The minimum allowed length for data in this form field.

fieldFormatMaxLength The maximum allowed length for data in this form field.

fieldFormatCharMapPCRE Form field value allowed character map.

valueType Learnt field value type

value Learnt field value

hits Learnt entity hit count

data Learned data.

devno count stateflag

export appfw learningdata

Export appfw learnt data in csv format to the location /var/learnt_data/

Synopsis

export appfw learningdata <profileName> <securityCheck>

Arguments

profileName Name of the profile.

securityCheck Name of the security check.

Possible values: startURL, cookieConsistency, fieldConsistency, crossSiteScripting, SQLInjection, fieldFormat, CSRFtag, XMLDoSCheck, XMLWSICheck, XMLAttachmentCheck, TotalXMLRequests, creditCardNumber, ContentType

target Target filename for data to be exported.

appfw-learningsettings

The following operations can be performed on "appfw-learningsettings":

unset| show| set|

unset appfw learningsettings

Use this command to remove appfw learningsettings settings.Refer to the set appfw learningsettings command for meanings of the arguments.

Synopsis

unset appfw learningsettings <profileName>

show appfw learningsettings

Displays the current application firewall learning settings for the specified profile. If no profile is specified, displays the current application firewall settings for all profiles on the Citrix ADC.

Synopsis

show appfw learningsettings

Arguments

profileName Name of the profile.

Output

startURLMinThreshold Minimum number of application firewall sessions that the learning engine must observe to learn start URLs.

startURLPercentThreshold Minimum percentage of application firewall sessions that must contain a particular start URL pattern for the learning engine to learn that start URL.

cookieConsistencyMinThreshold Minimum number of application firewall sessions that the learning engine must observe to learn cookies.

cookieConsistencyPercentThreshold Minimum percentage of application firewall sessions that must contain a particular cookie pattern for the learning engine to learn that cookie.

CSRFtagMinThreshold Minimum number of application firewall sessions that the learning engine must observe to learn cross-site request forgery (CSRF) tags.

CSRFtagPercentThreshold Minimum percentage of application firewall sessions that must contain a particular CSRF tag for the learning engine to learn that CSRF tag.

fieldConsistencyMinThreshold Minimum number of application firewall sessions that the learning engine must observe to learn field consistency information.

fieldConsistencyPercentThreshold Minimum percentage of application firewall sessions that must contain a particular field consistency pattern for the learning engine to learn that field consistency pattern.

crossSiteScriptingMinThreshold Minimum number of application firewall sessions that the learning engine must observe to learn HTML cross-site scripting patterns.

crossSiteScriptingPercentThreshold Minimum percentage of application firewall sessions that must contain a particular cross-site scripting pattern for the learning engine to learn that cross-site scripting pattern.

SQLInjectionMinThreshold Minimum number of application firewall sessions that the learning engine must observe to learn HTML SQL injection patterns.

SQLInjectionPercentThreshold Minimum percentage of application firewall sessions that must contain a particular HTML SQL injection pattern for the learning engine to learn that HTML SQL injection pattern.

fieldFormatMinThreshold Minimum number of application firewall sessions that the learning engine must observe to learn field formats.

fieldFormatPercentThreshold Minimum percentage of application firewall sessions that must contain a particular web form field pattern for the learning engine to recommend a field format for that form field.

CreditCardNumberMinThreshold Minimum threshold to learn Credit Card information.

CreditCardNumberPercentThreshold Minimum threshold in percent to learn Credit Card information.

ContentTypeMinThreshold Minimum threshold to learn Content Type information.

ContentTypePercentThreshold Minimum threshold in percent to learn Content Type information.

XMLWSIMinThreshold Minimum threshold to learn XML Web Services Interoperability.

XMLWSIPercentThreshold Minimum threshold (in percent) to learn XML Web Services Interoperability.

XMLAttachmentMinThreshold Minimum threshold to learn XML Attachments.

XMLAttachmentPercentThreshold Minimum threshold (in percent) to learn XML Attachments.

crossSiteScriptingAutoDeployGracePeriod The number of minutes after the threshold hit alert the learned rule will be deployed

SQLInjectionAutoDeployGracePeriod The number of minutes after the threshold hit alert the learned rule will be deployed

fieldFormatAutoDeployGracePeriod The number of minutes after the threshold hit alert the learned rule will be deployed

startURLAutoDeployGracePeriod The number of minutes after the threshold hit alert the learned rule will be deployed

cookieConsistencyAutoDeployGracePeriod The number of minutes after the threshold hit alert the learned rule will be deployed

CSRFtagAutoDeployGracePeriod The number of minutes after the threshold hit alert the learned rule will be deployed

fieldConsistencyAutoDeployGracePeriod The number of minutes after the threshold hit alert the learned rule will be deployed

ContentTypeAutoDeployGracePeriod The number of minutes after the threshold hit alert the learned rule will be deployed

devno count stateflag

set appfw learningsettings

Configures the application firewall learning settings for the specified profile.

Synopsis

set appfw learningsettings <profileName>

Arguments

profileName Name of the profile.

startURLMinThreshold Minimum number of application firewall sessions that the learning engine must observe to learn start URLs. Default value: 1 Minimum value: 1

startURLPercentThreshold Minimum percentage of application firewall sessions that must contain a particular start URL pattern for the learning engine to learn that start URL. Default value: 0 Minimum value: 0 Maximum value: 100

cookieConsistencyMinThreshold Minimum number of application firewall sessions that the learning engine must observe to learn cookies. Default value: 1 Minimum value: 1

cookieConsistencyPercentThreshold Minimum percentage of application firewall sessions that must contain a particular cookie pattern for the learning engine to learn that cookie. Default value: 0 Minimum value: 0 Maximum value: 100

CSRFtagMinThreshold Minimum number of application firewall sessions that the learning engine must observe to learn cross-site request forgery (CSRF) tags. Default value: 1 Minimum value: 1

CSRFtagPercentThreshold Minimum percentage of application firewall sessions that must contain a particular CSRF tag for the learning engine to learn that CSRF tag. Default value: 0 Minimum value: 0 Maximum value: 100

fieldConsistencyMinThreshold Minimum number of application firewall sessions that the learning engine must observe to learn field consistency information. Default value: 1 Minimum value: 1

fieldConsistencyPercentThreshold Minimum percentage of application firewall sessions that must contain a particular field consistency pattern for the learning engine to learn that field consistency pattern. Default value: 0 Minimum value: 0 Maximum value: 100

crossSiteScriptingMinThreshold Minimum number of application firewall sessions that the learning engine must observe to learn HTML cross-site scripting patterns. Default value: 1 Minimum value: 1

crossSiteScriptingPercentThreshold Minimum percentage of application firewall sessions that must contain a particular cross-site scripting pattern for the learning engine to learn that cross-site scripting pattern. Default value: 0 Minimum value: 0 Maximum value: 100

SQLInjectionMinThreshold Minimum number of application firewall sessions that the learning engine must observe to learn HTML SQL injection patterns. Default value: 1 Minimum value: 1

SQLInjectionPercentThreshold Minimum percentage of application firewall sessions that must contain a particular HTML SQL injection pattern for the learning engine to learn that HTML SQL injection pattern. Default value: 0 Minimum value: 0 Maximum value: 100

fieldFormatMinThreshold Minimum number of application firewall sessions that the learning engine must observe to learn field formats. Default value: 1 Minimum value: 1

fieldFormatPercentThreshold Minimum percentage of application firewall sessions that must contain a particular web form field pattern for the learning engine to recommend a field format for that form field. Default value: 0 Minimum value: 0 Maximum value: 100

CreditCardNumberMinThreshold Minimum threshold to learn Credit Card information. Default value: 1 Minimum value: 1

CreditCardNumberPercentThreshold Minimum threshold in percent to learn Credit Card information. Default value: 0 Minimum value: 0 Maximum value: 100

ContentTypeMinThreshold Minimum threshold to learn Content Type information. Default value: 1 Minimum value: 1

ContentTypePercentThreshold Minimum threshold in percent to learn Content Type information. Default value: 0 Minimum value: 0 Maximum value: 100

XMLWSIMinThreshold Minimum number of application firewall sessions that the learning engine must observe to learn web services interoperability (WSI) information. Default value: 1 Minimum value: 1

XMLWSIPercentThreshold Minimum percentage of application firewall sessions that must contain a particular pattern for the learning engine to learn a web services interoperability (WSI) pattern. Default value: 0 Minimum value: 0 Maximum value: 100

XMLAttachmentMinThreshold Minimum number of application firewall sessions that the learning engine must observe to learn XML attachment patterns. Default value: 1 Minimum value: 1

XMLAttachmentPercentThreshold Minimum percentage of application firewall sessions that must contain a particular XML attachment pattern for the learning engine to learn that XML attachment pattern. Default value: 0 Minimum value: 0 Maximum value: 100

fieldFormatAutoDeployGracePeriod The number of minutes after the threshold hit alert the learned rule will be deployed Default value: 10080 Minimum value: 5 Maximum value: 43200

SQLInjectionAutoDeployGracePeriod The number of minutes after the threshold hit alert the learned rule will be deployed Default value: 10080 Minimum value: 5 Maximum value: 43200

crossSiteScriptingAutoDeployGracePeriod The number of minutes after the threshold hit alert the learned rule will be deployed Default value: 10080 Minimum value: 5 Maximum value: 43200

startURLAutoDeployGracePeriod The number of minutes after the threshold hit alert the learned rule will be deployed Default value: 10080 Minimum value: 5 Maximum value: 43200

cookieConsistencyAutoDeployGracePeriod The number of minutes after the threshold hit alert the learned rule will be deployed Default value: 10080 Minimum value: 5 Maximum value: 43200

CSRFtagAutoDeployGracePeriod The number of minutes after the threshold hit alert the learned rule will be deployed Default value: 10080 Minimum value: 5 Maximum value: 43200

fieldConsistencyAutoDeployGracePeriod The number of minutes after the threshold hit alert the learned rule will be deployed Default value: 10080 Minimum value: 5 Maximum value: 43200

ContentTypeAutoDeployGracePeriod The number of minutes after the threshold hit alert the learned rule will be deployed Default value: 10080 Minimum value: 5 Maximum value: 43200

appfw-multipartFormContentType

The following operations can be performed on "appfw-multipartFormContentType":

add| rm| show|

add appfw multipartFormContentType

Add multipart form content type. This will classify a request/response with the specified content type as multipart form

Synopsis

add appfw multipartFormContentType <MultipartFormContenttypevalue>

Arguments

MultipartFormContenttypevalue Content type to be classified as multipart form

isRegex Is multipart_form content type a regular expression?

Possible values: REGEX, NOTREGEX Default value: NOTREGEX

rm appfw multipartFormContentType

Remove multipart form content type.

Synopsis

rm appfw multipartFormContentType <MultipartFormContenttypevalue>

Arguments

MultipartFormContenttypevalue Content type to be classified as multipart form

show appfw multipartFormContentType

Display all multipart form content types.

Synopsis

show appfw multipartFormContentType

Arguments

MultipartFormContenttypevalue Content type to be classified as multipart form

Output

isRegex Is multipart_form content type a regular expression?

builtin Flag to determine if multipart form contenttype is built-in or not

feature The feature to be checked while applying this config

devno count stateflag

appfw-policy

The following operations can be performed on "appfw-policy":

stat| rename| add| unset| rm| set| show|

stat appfw policy

Displays statistics for the specified application firewall policy. If no application firewall policy is specified, displays abbreviated statistics for all application firewall policies.

Synopsis

stat appfw policy

Arguments

name Name of the application firewall policy.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Policy undef hits (Undefhits) Number of undef hits on the policy

Example

stat appfw policy

Related Commands

- stat appfw policylabel

rename appfw policy

Renames an application firewall policy.

Synopsis

rename appfw policy <name>@ <newName>@

Arguments

name Existing name of the application firewall policy.

newName New name for the policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

Example

rename appfw policy oldname newname

add appfw policy

Creates an application firewall policy.

Synopsis

add appfw policy <name> <rule> <profileName>

Arguments

name Name for the policy. Must begin with a letter, number, or the underscore character \(_\), and must contain only letters, numbers, and the hyphen \(-\), period \(.\) pound \(#\), space \(\), at (@), equals \(=\), colon \(:\), and underscore characters. Can be changed after the policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my policy" or 'my policy'\).

rule Name of the Citrix ADC named rule, or a Citrix ADC expression, that the policy uses to determine whether to filter the connection through the application firewall with the designated profile.

profileName Name of the application firewall profile to use if the policy matches.

comment Any comments to preserve information about the policy for later reference.

logAction Where to log information for connections that match this policy.

unset appfw policy

Removes the settings of an existing application firewall policy. Attributes for which a default value is available revert to their default values. See the set appfw policy command for a description of the parameters..Refer to the set appfw policy command for meanings of the arguments.

Synopsis

unset appfw policy <name>

Example

unset appfw policy pol9 -undefAction

rm appfw policy

Removes an application firewall policy.

Synopsis

rm appfw policy <name>

Arguments

name Name of the policy to remove.

set appfw policy

Modifies the specified parameters of an application firewall policy.

Synopsis

set appfw policy <name>

Arguments

name Name of the policy to modify.

rule Name of the Citrix ADC named rule, or a Citrix ADC expression, that the policy uses to determine whether to filter the connection through the application firewall with the designated profile.

profileName Name of the application firewall profile to use if the policy matches.

comment Any comments to preserve information about the policy for later reference.

logAction Where to log information for connections that match this policy.

Example

set appfw policy pol9 -rule "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh2\\")"

show appfw policy

Displays the current settings for the specified application firewall policy. If no policy name is provided, displays a list of all application firewall policies currently configured on the Citrix ADC.

Synopsis

show appfw policy

Arguments

name Name of the policy.

Output

stateflag rule Name of the Citrix ADC named rule, or a Citrix ADC expression, that the policy uses to determine whether to filter the connection through the application firewall with the designated profile.

profileName Name of the application firewall profile to use if the policy matches.

hits Number of hits.

undefHits Number of Undef hits.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

comment Any comments to preserve information about the policy for later reference.

logAction Where to log information for connections that match this policy.

boundTo The entity name to which policy is bound

activePolicy Indicates whether policy is bound or not.

priority Specifies the priority of the policy.

bindPolicyType policyType vserverType policyType type builtin Flag to determine if application firewall policy is built-in or not

feature The feature to be checked while applying this config

devno count

appfw-policylabel

The following operations can be performed on "appfw-policylabel":

show| stat| rm| add| bind| rename| unbind|

show appfw policylabel

Displays the current settings for the specified application firewall policy label. If no policy label is specified, displays a list of all application firewall policy labels currently configured on the Citrix ADC.

Synopsis

show appfw policylabel

Arguments

labelName Name of the application firewall policy label.

Output

stateflag policylabeltype Type of transformations allowed by the policies bound to the label. Always http_req for application firewall policy labels.

numpol Number of polices bound to label.

hits Number of times policy label was invoked.

policyName Name of the application firewall policy to bind to the policy label.

priority Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Must be unique within a group of policies that are bound to the same bind point or label. Policies are evaluated in the order of their priority numbers.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

labelType Type of policy label to invoke if the current policy evaluates to TRUE and the invoke parameter is set. Available settings function as follows:

- reqvserver. Invoke the unnamed policy label associated with the specified request virtual server.
- policylabel. Invoke the specified user-defined policy label.

labelName Name of the policy label to invoke if the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is set to Policy Label.

description Description of the policylabel

flags policyType devno count

Example

i)show appfw policylabel appfw_label ii)show appfw policylabel

stat appfw policylabel

Displays statistics for the specified application firewall policy label. If no application firewall policy label is specified, displays abbreviated statistics for all application firewall policy labels.

Synopsis

stat appfw policylabel

Arguments

labelName Name of the application firewall policy label.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy Label Hits (Hits) Number of times policy label was invoked.

Related Commands

- stat appfw profile

rm appfw policylabel

Removes the specified application firewall policy label.

Synopsis

rm appfw policylabel <labelName>

Arguments

labelName Name of the application firewall policy label to remove.

Example

rm appfw policylabel appfw_label

add appfw policylabel

Creates a user-defined application firewall policy label.

Synopsis

add appfw policylabel <labelName> <policylabeltype>

Arguments

labelName Name for the policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the policy label is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy label" or 'my policy label').

policylabeltype Type of transformations allowed by the policies bound to the label. Always http_req for application firewall policy labels.

Possible values: http_req, httpquic_req

Example

add appfw policylabel appfw_label http_req

bind appfw policylabel

Binds the specified application firewall policy to the specified policy label.

Synopsis

bind appfw policylabel <labelName> <policyName> <priority>

Arguments

labelName Name of the application firewall policy label.

policyName Name of the application firewall policy to bind to the policy label.

priority Priority with which the policy is to be bound. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is smaller than the current policy's priority number.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

labelType Type of policy label to invoke if the current policy evaluates to TRUE and the invoke parameter is set. Available settings function as follows:

- reqvserver. Invoke the unnamed policy label associated with the specified request virtual server.
- policylabel. Invoke the specified user-defined policy label.

Possible values: reqvserver, policylabel

labelName Name of the policy label to invoke if the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is set to Policy Label.

Example

i)bind appfw policylabel trans_http_url pol_1 1 2 -invoke reqvserver CURRENT ii)bind appfw policylabel trans_http_url pol_2 2

rename appfw policylabel

Renames an application firewall policy label.

Synopsis

rename appfw policylabel <labelName>@ <newName>@

Arguments

labelName Existing name of the application firewall policy label.

newName The new name of the application firewall policylabel.

Example

rename appfw policylabel oldname newname

unbind appfw policylabel

Unbinds the specified application firewall policy from the specified policy label. See the bind appfw policylabel command for descriptions of the parameters.

Synopsis

unbind appfw policylabel <labelName> <policyName>

Arguments

labelName Name for the policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the policy label is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy label" or 'my policy label').

policyName Name of the application firewall policy to bind to the policy label.

priority Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind appfw policylabel appfw_label

appfw-profile

The following operations can be performed on "appfw-profile":

unset| bind| set| restore| add| archive| rm| show| unbind| stat|

unset appfw profile

Use this command to remove appfw profile settings.Refer to the set appfw profile command for meanings of the arguments.

Synopsis

unset appfw profile <name>

bind appfw profile

Binds the specified exemption (relaxation) or rule to the specified application firewall profile. NOTE: You should not attempt to bind more than one exemption or rule at a time by using this command.

Synopsis

bind appfw profile <name> ((-startURL <expression>) | -denyURL <expression> | (-fieldConsistency <string> <formActionURL>) | (-cookieConsistency <string>) | (-SQLInjection <string> <formActionURL> [-valueType <valueType> <valueExpression>]) | (-CMDInjection <string> <formActionURL> [-valueType (Keyword | SpecialString) <valueExpression>]) | (-CSRFTag <expression> <CSRFFormActionURL>) | (-crossSiteScripting <string> <formActionURL> [-valueType <valueType> <valueExpression>]) | (-fieldFormat <string> <formActionURL> <fieldType>) | (-safeObject <string> <expression> <maxMatchLength>) | -trustedLearningClients <ip_addr|ipv6_addr> | (-JSONSQLURL <expression> [-key <expression> [-valueType <valueType> <valueExpression>]]) | (-JSONCMDURL <expression> [-key <expression> [-valueType (Keyword | SpecialString) <valueExpression>]]) | (-JSONXSSURL <expression> [-key <expression> [-valueType <valueType> <valueExpression>]]) | (-JSONDoSURL <expression> [-JSONMaxContainerDepthCheck (ON | OFF)] [-JSONMaxDocumentLengthCheck (ON | OFF)] [-JSONMaxObjectKeyCountCheck (ON | OFF)] [-JSONMaxObjectKeyLengthCheck (ON | OFF)] [-JSONMaxArrayLengthCheck (ON | OFF)] [-JSONMaxStringLengthCheck (ON | OFF)]) | (-XMLDoSURL <expression> [-XMLMaxElementDepthCheck (ON | OFF)] [-XMLMaxElementNameLengthCheck (ON | OFF)] [-XMLMaxElementsCheck (ON | OFF)] [-XMLMaxElementChildrenCheck (ON | OFF)] [-XMLMaxNodesCheck (ON | OFF)] [-XMLMaxAttributesCheck (ON | OFF)] [-XMLMaxAttributeNameLengthCheck (ON | OFF)] [-XMLMaxAttributeValueLengthCheck (ON | OFF)] [-XMLMaxCharDATALengthCheck (ON | OFF)] [-XMLMaxFileSizeCheck (ON | OFF)] [-XMLMinFileSizeCheck (ON | OFF)] [-XMLMaxEntityExpansionsCheck (ON | OFF)] [-XMLMaxEntityExpansionDepthCheck (ON | OFF)] [-XMLMaxNamespacesCheck (ON | OFF)] [-XMLMaxNamespaceUriLengthCheck (ON | OFF)] [-XMLSOAPArrayCheck (ON | OFF)]) | (-XMLWSIURL <expression>) | (-XMLValidationURL <expression> (-XMLRequestSchema <string> | (-XMLWSDL <string>) | -XMLValidateSOAPEnvelope (ON | OFF))) | (-XMLAttachmentURL <expression> [-XMLMaxAttachmentSizeCheck (ON | OFF)] [-XMLAttachmentContentTypeCheck (ON | OFF)]) | (-XMLSQLInjection <string>) | (-XMLXSS <string>) | -contentType <expression> | -excludeResContentType <expression> | (-CreditCardNumber <expression> <CreditCardNumberUrl>) | (-logExpression <string> <expression>) | (-fileUploadType <expression> <formActionURL> -fileType <fileType> ...) | (-fakeAccount <expression> -tag <expression>) | (-confidField <string>) | (-blockKeyword <expression> -fieldName <expression> -formURL <expression>) | (-JSONBlockKeyword <expression> -key <expression> -JSONBlockkeywordURL <expression>) | (-bypasslist <expression> -valueType <valueType>) | (-denylist <expression> -valueType <valueType>))

Arguments

name Name of the profile to which to bind an exemption or rule.

startURL Add the specified URL to the start URL list. Enclose URLs in double quotes to ensure preservation of any embedded spaces or non-alphanumeric characters.

denyURL Add the specified URL to the deny URL list. Enclose URLs in double quotes to ensure preservation of any embedded spaces or non-alphanumeric characters.

fieldConsistency Exempt the specified web form field and form action URL from the form field consistency check, or exempt the specified cookie from the cookie consistency check. A form field consistency exemption (relaxation) consists of the following items:

- Web form field name. Name of the form field to exempt from this check.
- Form action URL. Action URL for the web form.
- IsRegex flag. The IsRegex flag, followed by YES if the form action URL is a regular expression, or NO if it is a literal string.

formActionURL Form action URL.

isRegex Is a regular expression?

Possible values: REGEX, NOTREGEX

cookieConsistency A cookie consistency exemption (relaxation) consists of the following items:

- Cookie name. Name of the cookie to exempt from this check.
- IsRegex flag. The IsRegex flag, followed by YES if the cookie name is a regular expression, or NO if it is a literal string.

isRegex Is a regular expression?

Possible values: REGEX, NOTREGEX

SQLInjection Exempt the specified HTTP header, web form field and the form action URL, or cookie from the SQL injection check. An SQL injection exemption (relaxation) consists of the following items: *Item name. Name of the web form field, cookie, or HTTP header to exempt from this check.

- Form action URL. If the item to be exempted is a web form field, the action URL for the web form.

- IsRegex flag. The IsRegex flag, followed by YES if the name or form action URL is a regular expression, or NO if it is a literal string.
- Location. Location that should be examined by the SQL injection check, either FORMFIELD for web form field, HEADER for HTTP header, or COOKIE for cookie.

formActionURL Form action URL for exceptions in fields, or request URL for exceptions in headers and cookies.

isRegex Is a regular expression?

Possible values: REGEX, NOTREGEX

location Location of SQL injection exception - form field, header or cookie.

Possible values: FORMFIELD, HEADER, COOKIE

valueType SQL value type. (Keyword | SpecialString | Wildchar | None

Possible values: Keyword, SpecialString, Wildchar

valueExpression SQL value expressions consistituting expressions for Keyword, SpecialString and Wildchars.

isValueRegex Is a regular expression?

Possible values: REGEX, NOTREGEX

CMDInjection Exempt the specified HTTP header, web form field and the form action URL, or cookie from the command injection check. A command injection exemption (relaxation) consists of the following items: *Item name. Name of the web form field, cookie, or HTTP header to exempt from this check.

- Form action URL. If the item to be exempted is a web form field, the action URL for the web form.
- IsRegex flag. The IsRegex flag, followed by YES if the name or form action URL is a regular expression, or NO if it is a literal string.
- Location. Location that should be examined by the CMD injection check, either FORMFIELD for web form field, HEADER for HTTP header, or COOKIE for cookie.

formActionURL Form action URL for exceptions in fields, or request URL for exceptions in headers and cookies.

isRegex Is a regular expression?

Possible values: REGEX, NOTREGEX

location Location of command injection exception - form field, header or cookie.

Possible values: FORMFIELD, HEADER, COOKIE

valueType Command value type. (Keyword | SpecialString)

Possible values: Keyword, SpecialString

valueExpression CMD value expressions consistituting expressions for Keyword and SpecialString

isValueRegex Is a regular expression?

Possible values: REGEX, NOTREGEX

CSRFTag Exempt the specified form field and web form from the cross-site request forgery (CSRF tagging) check. A CSRF tagging exemption (relaxation) consists of the following items:

- Web form field name. Regular expression that describes the web form field to exempt from this check.
- Form action URL. The action URL for the web form.

CSRFFormActionURL CSRF form action URL.

crossSiteScripting Exempt the specified string, found in the specified HTTP header, cookie, url or web form, from the cross-site scripting check. A cross-site scripting check exemption (relaxation) consists of the following items:

- HTML to exempt. The string to exempt from the cross-site scripting check.
- URL. The URL to exempt.
- IsRegex flag. The IsRegex flag, followed by YES if the URL is a regular expression, or NO if it is a literal string.
- location. Location which should be examined by the cross-site scripting check, either FORMFIELD for web form field, HEADER for HTTP header, COOKIE for cookie, or URL for complete url

formActionURL Form action URL for exceptions in fields, or request URL for exceptions in headers, cookies or url.

isRegex Is a regular expression?

Possible values: REGEX, NOTREGEX

location Location of cross-site scripting exception - form field, header, cookie or URL.

Possible values: FORMFIELD, HEADER, COOKIE, URL

valueType XSS value type. (Tag | Attribute | Pattern)

Possible values: Tag, Attribute, Pattern

valueExpression XSS value expressions consistituting expressions for Tag, Attribute and Pattern.

isValueRegex Is a regular expression?

Possible values: REGEX, NOTREGEX

fieldFormat Impose the specified format on content returned by users in the specified web form field. A field format rule consists of the following items:

- Form field name. The name of the form field.
- Form action URL. The form action URL for the web form.
- Field type. The field type (format) to enforce on the specified web form field.
- Field format minimum length. The minimum length allowed for data in the specified field. If 0, field can be left blank.
- Field format maximum length. The maximum length allowed for data in the specified field.
- IsRegex flag. The IsRegex flag, followed by YES if the URL is a regular expression, or NO if it is a literal string.

formActionURL Form action URL.

fieldType Field type.

fieldFormatMinLength Field format minimum length. Default value: 0 Minimum value: 0 Maximum value: 2147483647

fieldFormatMaxLength Field format maximum length. Default value: 65535 Minimum value: 1 Maximum value: 2147483647

isRegex Is a regular expression?

Possible values: REGEX, NOTREGEX

safeObject Protect web sites from exposing sensitive private information such as social security numbers, credit card numbers, driver's license numbers, passport numbers, and any other type of private information that can be described by a regular expression. A safe object consists of the following items:

- Name. A name that describes the type of information that the safe object is to protect.
- Expression. PCRE-format regular expression that describes the information to be protected.
- Maximum match length. Maximum length of a matched string.
- Action. "X-Out" to mask blocked information with the letter X, or "Remove" to remove the information.

expression Safe Object regular expression.

maxMatchLength Maximum match length for a Safe Object expression. Default value: 1 Minimum value: 1 Maximum value: 65535

action Safe Object action types. (BLOCK | LEARN | LOG | STATS | NONE)

trustedLearningClients Trusted host/network learning IP. This binding is applicable to profile Type: HTML, XML.

comment Any comments about the purpose of profile, or other useful information about the profile.

state Enabled.

Possible values: ENABLED, DISABLED Default value: ENABLED

JSONSQLURL A regular expression that designates a URL on the Json SQL URL list for which SQL violations are relaxed. Enclose URLs in double quotes to ensure preservation of any embedded spaces or non-alphanumeric characters.

key JSON SQL Key name

isRegex Is a regular expression?

Possible values: REGEX, NOTREGEX

valueType JSON SQL key value type. (Keyword | SpecialString)

Possible values: Keyword, SpecialString, Wildchar

valueExpression JSON_SQL key value expressions consistituting expressions for Keyword and SpecialString

isValueRegex Is a regular expression?

Possible values: REGEX, NOTREGEX

JSONCMDURL A regular expression that designates a URL on the Json CMD URL list for which Command injection violations are relaxed. Enclose URLs in double quotes to ensure preservation of any embedded spaces or non-alphanumeric characters.

key JSON CMD Key name

isRegex Is a regular expression?

Possible values: REGEX, NOTREGEX

valueType JSON Command key value type. (Keyword | SpecialString)

Possible values: Keyword, SpecialString

valueExpression JSON_CMD key value expressions consistituting expressions for Keyword and SpecialString

isValueRegex Is a regular expression?

Possible values: REGEX, NOTREGEX

JSONXSSURL A regular expression that designates a URL on the Json XSS URL list for which XSS violations are relaxed. Enclose URLs in double quotes to ensure preservation of any embedded spaces or non-alphanumeric characters.

key JSON XSS Key name

isRegex Is a regular expression?

Possible values: REGEX, NOTREGEX

valueType JSON Command key value type. (Keyword | SpecialString)

Possible values: Tag, Attribute, Pattern

valueExpression JSON_XSS key value expressions consistituting expressions for Keyword and SpecialString

isValueRegex Is a regular expression?

Possible values: REGEX, NOTREGEX

JSONDoSURL The URL on which we need to enforce the specified JSON denial-of-service (JSONDoS) attack protections. An JSON DoS configuration consists of the following items:

- URL. PCRE-format regular expression for the URL.
- Maximum-document-length-check toggle. ON to enable this check, OFF to disable it.
- Maximum document length. Positive integer representing the maximum length of the JSON document.
- Maximum-container-depth-check toggle. ON to enable, OFF to disable.
- Maximum container depth. Positive integer representing the maximum container depth of the JSON document.
- Maximum-object-key-count-check toggle. ON to enable, OFF to disable.
- Maximum object key count. Positive integer representing the maximum allowed number of keys in any of the JSON object.
- Maximum-object-key-length-check toggle. ON to enable, OFF to disable.
- Maximum object key length. Positive integer representing the maximum allowed length of key in any of the JSON object.
- Maximum-array-value-count-check toggle. ON to enable, OFF to disable.
- Maximum array value count. Positive integer representing the maximum allowed number of values in any of the JSON array.
- Maximum-string-length-check toggle. ON to enable, OFF to disable.
- Maximum string length. Positive integer representing the maximum length of string in JSON.

JSONMaxContainerDepthCheck State if JSON Max Container Depth Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

JSONMaxContainerDepth Maximum allowed nesting depth of JSON document. JSON allows one to nest the containers (object and array) in any order to any depth. This check protects against documents that have excessive depth of hierarchy. Default value: 5 Minimum value: 0 Maximum value: 127

JSONMaxDocumentLengthCheck State if JSON Max Document Length Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

JSONMaxDocumentLength Maximum document length of JSON document, in bytes. Default value: 20000000 Minimum value: 0 Maximum value: 2147483647

JSONMaxObjectKeyCountCheck State if JSON Max Object Key Count Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

JSONMaxObjectKeyCount Maximum key count in the any of JSON object. This check protects against objects that have large number of keys. Default value: 10000 Minimum value: 0 Maximum value: 2147483647

JSONMaxObjectKeyLengthCheck State if JSON Max Object Key Length Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

JSONMaxObjectKeyLength Maximum key length in the any of JSON object. This check protects against objects that have large keys. Default value: 128 Minimum value: 0 Maximum value: 2147483647

JSONMaxArrayLengthCheck State if JSON Max Array Length Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

JSONMaxArrayLength Maximum array length in the any of JSON object. This check protects against arrays having large lengths. Default value: 10000 Minimum value: 0 Maximum value: 2147483647

JSONMaxStringLengthCheck State if JSON Max String Length Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

JSONMaxStringLength Maximum string length in the JSON. This check protects against strings that have large length. Default value: 1000000 Minimum value: 0 Maximum value: 2147483647

XMLDoSURL Exempt the specified URL from the specified XML denial-of-service (XDoS) attack protections. An XDoS exemption (relaxation) consists of the following items:

- URL. PCRE-format regular expression for the URL or URLs to be exempted.
- Maximum-element-depth-check toggle. ON to enable this check, OFF to disable it.
- Maximum-element-depth-check toggle. ON to enable, OFF to disable.
- Maximum-element-depth-check level. Positive integer representing the maximum allowed depth of nested XML elements.
- Maximum-element-name-length-check toggle. ON to enable, OFF to disable.
- Maximum element name length. Positive integer representing the maximum allowed length of XML element names.

- Maximum-number-of-elements-check toggle. ON to enable, OFF to disable.
- Maximum number of elements. Positive integer representing the maximum allowed number of XML elements.
- Maximum-number-of-element-children-check toggle. ON to enable, OFF to disable.
- Maximum number of element children. Positive integer representing the maximum allowed number of XML element children.
- Maximum-number-of-attributes-check toggle. ON to enable, OFF to disable.
- Maximum number of attributes. Positive integer representing the maximum allowed number of XML attributes.
- Maximum-attribute-name-length-check toggle. ON to enable, OFF to disable.
- Maximum attribute name length. Positive integer representing the maximum allowed length of XML attribute names.
- Maximum-attribute-value-length-check toggle. ON to enable, OFF to disable.
- Maximum attribute value length. Positive integer representing the maximum allowed length of XML attribute values.
- Maximum-character-data-length-check toggle. ON to enable, OFF to disable.
- Maximum character-data length. Positive integer representing the maximum allowed length of XML character data.
- Maximum-file-size-check toggle. ON to enable, OFF to disable.
- Maximum file size. Positive integer representing the maximum allowed size, in bytes. of attached or uploaded files.
- Minimum-file-size-check toggle. ON to enable, OFF to disable.
- Minimum file size. Positive integer representing the minimum allowed size, in bytes, of attached or uploaded files.
- Maximum-number-of-entity-expansions-check toggle. ON to enable, OFF to disable.
- Maximum number of entity expansions. Positive integer representing the maximum allowed number of XML entity expansions.
- Maximum-number-of XML-namespaces-check toggle. ON to enable, OFF to disable.
- Maximum number of XML namespaces. Positive integer representing the maximum allowed number of XML namespaces.
- Maximum-XML-namespace-URI-length-check toggle. ON to enable, OFF to disable.

- MaximumXML-namespace URI length. Positive integer representing the maximum allowed length of XML namespace URIs.
- Block-processing-instructions toggle. Block XML processing instructions. ON to enable, OFF to disable.
- Block-DTD toggle. Block design type documents (DTDs). ON to enable, OFF to disable.
- Block-external-XML-entitites toggle. ON to enable, OFF to disable.
- Maximum-SOAP-array-check toggle. ON to enable, OFF to disable.
- Maximum SOAP-array size. Positive integer representing the maximum allowed size of XML SOAP arrays.
- Maximum SOAP-array rank. Positive integer representing the maximum rank (dimensions) of any single XML SOAP array.

XMLMaxElementDepthCheck State if XML Max Element Depth Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

XMLMaxElementDepth Maximum nesting (depth) of XML elements. This check protects against documents that have excessive depth of hierarchy. Default value: 256 Minimum value: 1 Maximum value: 65535

XMLMaxElementNameLengthCheck State if XML Max Element Name Length Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

XMLMaxElementNameLength Specify the longest name of any element (including the prefix for qualified element name) to protect against overflow attacks. Default value: 128 Minimum value: 1 Maximum value: 65535

XMLMaxElementsCheck State if XML Max Elements Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

XMLMaxElements Specifying maximum number of elements protects against overflow attacks. Default value: 65535 Minimum value: 1 Maximum value: 65535

XMLMaxElementChildrenCheck State if XML Max Element Children Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

XMLMaxElementChildren Specifying maximum number of children allowed per element protects against overflow attacks. Default value: 65535 Minimum value: 0 Maximum value: 65535

XMLMaxNodesCheck State if XML Max Nodes Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

XMLMaxNodes Specify the maximum number of nodes. Protects against overflow attacks. Default value: 65535 Minimum value: 0 Maximum value: 65535

XMLMaxAttributesCheck State if XML Max Attributes Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

XMLMaxAttributes Specify maximum number of attributes per element. Protects against overflow attacks. Default value: 256 Minimum value: 0 Maximum value: 65535

XMLMaxAttributeNameLengthCheck State if XML Max Attribute Name Length Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

XMLMaxAttributeNameLength Specify the longest name of any attribute (including the prefix for qualified attribute name). Protects against overflow attacks. Default value: 128 Minimum value: 1 Maximum value: 65535

XMLMaxAttributeValueLengthCheck State if XML Max Atribute Value Length is ON or OFF.

Possible values: ON, OFF Default value: OFF

XMLMaxAttributeValueLength Specify the longest value of any attribute. Protects against overflow attacks. Default value: 2048 Minimum value: 0 Maximum value: 65535

XMLMaxCharDATALengthCheck State if XML Max CDATA Length Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

XMLMaxCharDATALength Maximum size of CDATA protects against overflow attacks and large unparsed data within XML messages. Default value: 65535 Minimum value: 0 Maximum value: 1000000000

XMLMaxFileSizeCheck State if XML Max File Size Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

XMLMaxFileSize Maximum size of the XML messages protects against overflow attacks. Default value: 20000000 Minimum value: 4 Maximum value: 1000000000

XMLMinFileSizeCheck State if XML Min File Size Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

XMLMinFileSize Enforces minimum message size. Default value: 9 Minimum value: 4 Maximum value: 1000000000

XMLBlockPI State if XML Block PI is ON or OFF. Protects resources from denial of service attacks as SOAP messages can not have Processing Instruction (PI) in the message.

Possible values: ON, OFF Default value: OFF

XMLBlockDTD State if XML DTD is ON or OFF. Protects against recursive Document Type Declaration (DTD) entity expansion attacks. Also, SOAP messages can not have DTD in the message.

Possible values: ON, OFF Default value: OFF

XMLBlockExternalEntities State if XML Block External Entities Check is ON or OFF. Protects against XML External Entity (XXE) attacks that force applications to parse untrusted external entities (sources) in XML documents.

Possible values: ON, OFF Default value: OFF

XMLMaxEntityExpansionsCheck State if XML Max Entity Expansions Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

XMLMaxEntityExpansions Specify maximum allowed number of entity expansions. Protects aganist Entity Expansion Attack. Default value: 512 Minimum value: 0 Maximum value: 1024

XMLMaxEntityExpansionDepthCheck State if XML Max Entity Expansions Depth Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

XMLMaxEntityExpansionDepth Specify maximum entity expansion depth. Protects aganist Entity Expansion Attack. Default value: 8 Minimum value: 0 Maximum value: 24

XMLMaxNamespacesCheck State if XML Max Namespaces Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

XMLMaxNamespaces Specify maximum number of active namespaces. Protects against overflow attacks. Default value: 16 Minimum value: 0 Maximum value: 512

XMLMaxNamespaceUriLengthCheck State if XML Max Namspace URI Length Check is ON or OFF.

Possible values: ON, OFF Default value: OFF

XMLMaxNamespaceUriLength Specify the longest URI of any XML namespace. Protects against overflow attacks. Default value: 256 Minimum value: 0 Maximum value: 65535

XMLSOAPArrayCheck State if XML SOAP Array check is ON or OFF.

Possible values: ON, OFF Default value: OFF

XMLMaxSOAPArraySize XML Max Total SOAP Array Size. Protects against SOAP Array Abuse attack. Default value: 20000000 Minimum value: 0 Maximum value: 1000000000

XMLMaxSOAPArrayRank XML Max Total SOAP Array Rank. Protects against SOAP Array Abuse attack. Default value: 16 Minimum value: 0 Maximum value: 32

XMLWSIURL Exempt the specified URL from the web services interoperability (WS-I) check. The URL is specified as a PCRE-format regular expression, which can match one or more URLs.

XMLWSIChecks Synonym for XMLWISURL, but takes a literal URL instead of a PCRE-format regular expression.

XMLValidationURL Exempt the specified URL from the XML message validation check. An XML message validation exemption (relaxation) consists of the following items:

- URL. PCRE-format regular expression that matches the URL(s) to be exempted.
- XML-request-schema toggle. Use the specified XML schema to validate requests. ON to enable, OFF to disable.
- XML request schema. XML schema to use for validating requests.
- XML-response-schema toggle. Use the specified XML schema to validate responses. ON to enable, OFF to disable.
- XML response schema. XML schema to use for validating responses.
- WSDL toggle. Use the specified WSDL to validate. ON to enable, OFF to disable.
- WSDL. WSDL to use for validation.
- SOAP-envelope toggle. Validate against the SOAP envelope. ON to enable, OFF to disable.

- Additional-SOAP-headers toggle. Validate against the extended list of SOAP headers. ON to enable, OFF to disable.
- XML-end-point check. ABSOLUTE to use an absolute end point, RELATIVE to use a relative end point.

XMLRequestSchema XML Schema object for request validation .

XMLResponseSchema XML Schema object for response validation .

XMLWSDL WSDL object for soap request validation .

XMLAdditionalSOAPHeaders Allow addtional soap headers.

Possible values: ON, OFF

XMLEndPointCheck Modifies the behaviour of the Request URL validation w.r.t. the Service URL. If set to ABSOLUTE, the entire request URL is validated with the entire URL mentioned in Service of the associated WSDL. eg: Service URL: http://example.org/ExampleService, Request URL: http//example.com/ExampleService would FAIL the validation. If set to RELATIVE, only the non-hostname part of the request URL is validated against the non-hostname part of the Service URL. eg: Service URL: http://example.org/ExampleService, Request URL: http//example.com/ExampleService would PASS the validation.

Possible values: ABSOLUTE, RELATIVE Default value: ABSOLUTE

XMLValidateSOAPEnvelope Validate SOAP Evelope only.

Possible values: ON, OFF

XMLValidateResponse Validate response message.

Possible values: ON, OFF

XMLAttachmentURL Exempt the specified URL from the XML attachment check. An XML attachment exemption (relaxation) consists of the following items:

- URL. PCRE-format regular expression that matches the URL(s) to be exempted.
- Maximum-attachment-size-check toggle. ON to enable, OFF to disable.
- Maximum attachment size. Positive integer representing the maximum allowed size in bytes for each XML attachment.
- Attachment-content-type-check toggle. ON to enable, OFF to disable.

- Attachment content type. PCRE-format regular expression that specifies the list of MIME content types allowed for XML attachments.

XMLMaxAttachmentSizeCheck State if XML max attachment size check is ON or OFF. Protects against XML requests with large attachment data.

Possible values: ON, OFF Default value: OFF

XMLMaxAttachmentSize Specify maximum attachment size. Minimum value: 0 Maximum value: 1000000000

XMLAttachmentContentTypeCheck State if XML attachment content-type check is ON or OFF. Protects against XML requests with illegal attachments.

Possible values: ON, OFF Default value: OFF

XMLAttachmentContentType Specify content-type regular expression.

XMLSQLInjection Exempt the specified URL from the XML SQL injection check. An XML SQL injection exemption (relaxation) consists of the following items:

- Name. Name to exempt, as a string or a PCRE-format regular expression.
- ISREGEX flag. REGEX if URL is a regular expression, NOTREGEX if URL is a fixed string.
- Location. ELEMENT if the injection is located in an XML element, ATTRIBUTE if located in an XML attribute.

isRegex Is a regular expression?

Possible values: REGEX, NOTREGEX

location Location of SQL injection exception - XML Element or Attribute. Default location is 'ELEMENT'

Possible values: ELEMENT, ATTRIBUTE Default value: AS_XMLLOCATION_ELEMENT

XMLXSS Exempt the specified URL from the XML cross-site scripting (XSS) check. An XML cross-site scripting exemption (relaxation) consists of the following items:

- URL. URL to exempt, as a string or a PCRE-format regular expression.
- ISREGEX flag. REGEX if URL is a regular expression, NOTREGEX if URL is a fixed string.
- Location. ELEMENT if the attachment is located in an XML element, ATTRIBUTE if located in an XML attribute.

isRegex Is a regular expression?

Possible values: REGEX, NOTREGEX

location Location of XSS injection exception - XML Element or Attribute. Default location is 'ELEMENT'

Possible values: ELEMENT, ATTRIBUTE Default value: AS_XMLLOCATION_ELEMENT

contentType Add the specified content-type to the content-type list.Enclose content-type in double quotes to ensure preservation of any embedded spaces or non-alphanumeric characters.

excludeResContentType Add the specified content-type to the response content-type list that are to be excluded from inspection. Enclose content-type in double quotes to ensure preservation of any embedded spaces or non-alphanumeric characters.

CreditCardNumber Add expression to the list of object expression which are to be bypassed from safe commerce checks.

CreditCardNumberUrl The url for which the list of credit card numbers are needed to be bypassed from inspection

logExpression Bind specified logExpression to application firewall profile

expression Log expression. Maximum value: 1500

fileUploadType Protect web sites from unknown file upload types.. A file upload object consists of the following items:

- Form field name. The name of the form field.
- Form action URL. The form action URL for the web form.
- File Type. Allowed file type.
- Content Type. Request Content Type.

formActionURL FileUploadTypes action URL.

isNameRegex Is field name a regular expression?

Possible values: REGEX, NOTREGEX

fileType FileUploadTypes file types.

isAutoDeployed Is the rule auto deployed by dynamic profile ?

Possible values: AUTODEPLOYED, NOTAUTODEPLOYED

resourceId A "id" that identifies the rule.

fakeAccount Add Fake Account Detection bind rule.

tag Fake account Form tag.

isFieldNameRegex Is Fake Account Detection field name regex?

Possible values: REGEX, NOTREGEX

formExpression A regular expression that defines the Fake Account.

formURL The fake account detection URL.

confidField Add confidential fields to the bindings. Form fields designated as confidential have the information that is provided in those fields x'd out in the audit logs

formURL URL of the web page that contains the web form.

isRegex Is Fake Account Detection field name regular expression?

Possible values: REGEX, NOTREGEX

blockKeyword Add block keyword bind rule.

fieldName A block keyword field name

formURL The blockkeyword form action URL.

isNameRegex Is block keyword field name regular expression?

Possible values: REGEX, NOTREGEX

blockKeywordType block keyword type(literal|PCRE)

Possible values: literal, PCRE

JSONBlockKeyword Add JSON block keyword bind rule.

key JSON block keyword keyname

JSONBlockkeywordURL The json blockkeyword URL.

isRegex Is JSON blockkeyword key a regular expression?

Possible values: REGEX, NOTREGEX

JSONBlockKeywordType JSON block keyword type

Possible values: literal, PCRE

bypasslist Add bypass list rule.

valueType Bypass List value type

Possible values: literal, PCRE, Expression

ruleAction Bypass List Action

Possible values: none, log

location Bypass List scan location

Possible values: IPv4, IPv6, URL

denylist Add deny list rule.

valueType Deny List value type

Possible values: literal, PCRE, Expression

ruleAction Deny List Action. Default value = REDIRECT

location Deny List scan location

Possible values: IPv4, IPv6, URL

RuleType Specifies rule type of binding

Possible values: ALLOW, DENY

set appfw profile

Modifies the specified parameters of the specified application firewall profile.

Synopsis

set appfw profile <name>

Arguments

name Name of the profile that you want to modify.

startURLAction One or more Start URL actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -startURLaction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -startURLaction none". Default value: AS_DEFAULT_DISPOSITION

inferContentTypeXmlPayloadAction One or more infer content type payload actions. Available settings function as follows:

- Block - Block connections that have mismatch in content-type header and payload.
- Log - Log connections that have mismatch in content-type header and payload. The mismatched content-type in HTTP request header will be logged for the request.
- Stats - Generate statistics when there is mismatch in content-type header and payload.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -inferContentTypeXMLPayloadAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -inferContentTypeXMLPayloadAction none". Please note "none" action cannot be used with any other action type. Default value: AS_INFER_CONTENT_TYPE_XML_PAYLOAD_DEFAULT_DISPOSITION

contentTypeAction One or more Content-type actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -contentTypeaction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -contentTypeaction none". Default value: AS_DEFAULT_CONTENT_TYPE_DISPOSITION

inspectContentTypes One or more InspectContentType lists.

- application/x-www-form-urlencoded
- multipart/form-data
- text/x-gwt-rpc

CLI users: To enable, type "set appfw profile -InspectContentTypes" followed by the content types to be inspected. Default value: AS_DEFAULT_INSPECTION_CONTENT_TYPE

startURLClosure Toggle the state of Start URL Closure.

Possible values: ON, OFF Default value: OFF

denyURLAction One or more Deny URL actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

NOTE: The Deny URL check takes precedence over the Start URL check. If you enable blocking for the Deny URL check, the application firewall blocks any URL that is explicitly blocked by a Deny URL, even if the same URL would otherwise be allowed by the Start URL check.

CLI users: To enable one or more actions, type "set appfw profile -denyURLaction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -denyURLaction none". Default value: AS_DEFAULT_DISPOSITION

RefererHeaderCheck Enable validation of Referer headers. Referer validation ensures that a web form that a user sends to your web site originally came from your web site, not an outside attacker. Although this parameter is part of the Start URL check, referer validation protects against cross-site request forgery (CSRF) attacks, not Start URL attacks.

Possible values: OFF, if_present, AlwaysExceptStartURLs, AlwaysExceptFirstRequest Default value: OFF

cookieConsistencyAction One or more Cookie Consistency actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.

- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -cookieConsistencyAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -cookieConsistencyAction none". Default value: none

cookieHijackingAction One or more actions to prevent cookie hijacking. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check. NOTE: Cookie Hijacking feature is not supported for TLSv1.3

CLI users: To enable one or more actions, type "set appfw profile -cookieHijackingAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -cookieHijackingAction none". Default value: none

cookieTransforms Perform the specified type of cookie transformation. Available settings function as follows:

- Encryption - Encrypt cookies.
- Proxying - Mask contents of server cookies by sending proxy cookie to users.
- Cookie flags - Flag cookies as HTTP only to prevent scripts on user's browser from accessing and possibly modifying them. CAUTION: Make sure that this parameter is set to ON if you are configuring any cookie transformations. If it is set to OFF, no cookie transformations are performed regardless of any other settings.

Possible values: ON, OFF

cookieEncryption Type of cookie encryption. Available settings function as follows:

- None - Do not encrypt cookies.
- Decrypt Only - Decrypt encrypted cookies, but do not encrypt cookies.
- Encrypt Session Only - Encrypt session cookies, but not permanent cookies.
- Encrypt All - Encrypt all cookies.

Possible values: none, decryptOnly, encryptSessionOnly, encryptAll Default value: none

cookieProxying Cookie proxy setting. Available settings function as follows:

- None - Do not proxy cookies.
- Session Only - Proxy session cookies by using the Citrix ADC session ID, but do not proxy permanent cookies.

Possible values: none, sessionOnly Default value: none

addCookieFlags Add HttpOnly and Secure flags to cookies

Possible values: none, httpOnly, secure, all Default value: none

fieldConsistencyAction One or more Form Field Consistency actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -fieldConsistencyaction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -fieldConsistencyAction none". Default value: none

CSRFtagAction One or more Cross-Site Request Forgery (CSRF) Tagging actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -CSRFTagAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -CSRFTagAction none". Default value: none

crossSiteScriptingAction One or more Cross-Site Scripting (XSS) actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -crossSiteScriptingAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -crossSiteScriptingAction none". Default value: AS_DEFAULT_DISPOSITION

crossSiteScriptingTransformUnsafeHTML Transform cross-site scripts. This setting configures the application firewall to disable dangerous HTML instead of blocking the request. CAUTION: Make sure that this parameter is set to ON if you are configuring any cross-site scripting transformations. If it is set to OFF, no cross-site scripting transformations are performed regardless of any other settings.

Possible values: ON, OFF

crossSiteScriptingCheckCompleteURLs Check complete URLs for cross-site scripts, instead of just the query portions of URLs.

Possible values: ON, OFF

SQLInjectionAction One or more HTML SQL Injection actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -SQLInjectionAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -SQLInjectionAction none". Default value: AS_DEFAULT_DISPOSITION

CMDInjectionAction Command injection action. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -cmdInjectionAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -cmdInjectionAction none". Default value: none

CMDInjectionType Available CMD injection types. -CMDSplChar : Checks for CMD Special Chars -CMDKeyword : Checks for CMD Keywords -CMDSplCharANDKeyword : Checks for both and blocks if both are found -CMDSplCharORKeyword : Checks for both and blocks if anyone is found, -None : Disables checking using both CMD Special Char and Keyword

Possible values: CMDSplChar, CMDKeyword, CMDSplCharORKeyword, CMDSplCharANDKeyword, None Default value: CMDSplCharANDKeyword

SQLInjectionTransformSpecialChars Transform injected SQL code. This setting configures the application firewall to disable SQL special strings instead of blocking the request. Since most SQL servers require a special string to activate an SQL keyword, in most cases a request that contains injected SQL code is safe if special strings are disabled. CAUTION: Make sure that this parameter is set to ON if you are configuring any SQL injection transformations. If it is set to OFF, no SQL injection transformations are performed regardless of any other settings.

Possible values: ON, OFF

SQLInjectionType Available SQL injection types. -SQLSplChar : Checks for SQL Special Chars -SQLKeyword : Checks for SQL Keywords -SQLSplCharANDKeyword : Checks for both and blocks if both are found -SQLSplCharORKeyword : Checks for both and blocks if anyone is found -None : Disables checking using both SQL Special Char and Keyword

Possible values: SQLSplChar, SQLKeyword, SQLSplCharORKeyword, SQLSplCharANDKeyword, None

SQLInjectionCheckSQLWildChars Check for form fields that contain SQL wild chars .

Possible values: ON, OFF

SQLInjectionGrammar Check for SQL injection using SQL grammar

Possible values: ON, OFF Default value: OFF

CMDInjectionGrammar Check for CMD injection using CMD grammar

Possible values: ON, OFF Default value: OFF

fieldFormatAction One or more Field Format actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of suggested web form fields and field format assignments.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -fieldFormatAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -fieldFormatAction none". Default value: AS_DEFAULT_DISPOSITION

defaultFieldFormatType Designate a default field type to be applied to web form fields that do not have a field type explicitly assigned to them.

defaultFieldFormatMinLength Minimum length, in characters, for data entered into a field that is assigned the default field type. To disable the minimum and maximum length settings and allow data of any length to be entered into the field, set this parameter to zero (0). Default value: 0 Minimum value: 0 Maximum value: 2147483647

defaultFieldFormatMaxLength Maximum length, in characters, for data entered into a field that is assigned the default field type. Default value: 65535 Minimum value: 1 Maximum value: 2147483647

bufferOverflowAction One or more Buffer Overflow actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -bufferOverflowAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -bufferOverflowAction none". Default value: AS_DEFAULT_DISPOSITION

grpcAction gRPC validation Default value: AS_DEFAULT_GRPC_DISPOSITION

restAction rest validation Default value: AS_DEFAULT_GRPC_DISPOSITION

bufferOverflowMaxURLLength Maximum length, in characters, for URLs on your protected web sites. Requests with longer URLs are blocked. Default value: 1024 Minimum value: 0 Maximum value: 65535

bufferOverflowMaxHeaderLength Maximum length, in characters, for HTTP headers in requests sent to your protected web sites. Requests with longer headers are blocked. Default value: 4096 Minimum value: 0 Maximum value: 65535

bufferOverflowMaxCookieLength Maximum length, in characters, for cookies sent to your protected web sites. Requests with longer cookies are blocked. Default value: 4096 Minimum value: 0 Maximum value: 65535

bufferOverflowMaxQueryLength Maximum length, in bytes, for query string sent to your protected web sites. Requests with longer query strings are blocked. Default value: 65535 Minimum value: 0 Maximum value: 65535

bufferOverflowMaxTotalHeaderLength Maximum length, in bytes, for the total HTTP header length in requests sent to your protected web sites. The minimum value of this and maxHeaderLen in httpProfile will be used. Requests with longer length are blocked. Default value: 65535 Minimum value: 0 Maximum value: 65535

creditCardAction One or more Credit Card actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -creditCardAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -creditCardAction none". Default value: none

creditCard Credit card types that the application firewall should protect. Default value: none

creditCardMaxAllowed This parameter value is used by the block action. It represents the maximum number of credit card numbers that can appear on a web page served by your protected

web sites. Pages that contain more credit card numbers are blocked. Minimum value: 0 Maximum value: 255

creditCardXOut Mask any credit card number detected in a response by replacing each digit, except the digits in the final group, with the letter "X."

Possible values: ON, OFF

doSecureCreditCardLogging Setting this option logs credit card numbers in the response when the match is found.

Possible values: ON, OFF

streaming Setting this option converts content-length form submission requests (requests with content-type "application/x-www-form-urlencoded" or "multipart/form-data") to chunked requests when atleast one of the following protections : Signatures, SQL injection protection, XSS protection, form field consistency protection, starturl closure, CSRF tagging, JSON SQL, JSON XSS, JSON DOS is enabled. Please make sure that the backend server accepts chunked requests before enabling this option. Citrix recommends enabling this option for large request sizes(>20MB).

Possible values: ON, OFF

trace Toggle the state of trace

Possible values: ON, OFF

requestContentType Default Content-Type header for requests. A Content-Type header can contain 0-255 letters, numbers, and the hyphen (-) and underscore (_) characters. Default value: NS_S_AS_DEFAULT_REQUEST_CONTENT_TYPE

responseContentType Default Content-Type header for responses. A Content-Type header can contain 0-255 letters, numbers, and the hyphen (-) and underscore (_) characters. Default value: NS_S_AS_DEFAULT_RESPONSE_CONTENT_TYPE

JSONErrorObject Name to the imported JSON Error Object to be set on application firewall profile.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my JSON error object" or 'my JSON error object'\). Default value: NS_S_AS_ERROR_OBJECT_DEFAULT

JSONErrorStatusCode Response status code associated with JSON error page. Non-empty JSON error object must be imported to the application firewall profile for the status code. Default value: 200 Minimum value: 1 Maximum value: 999

JSONErrorStatusMessage Response status message associated with JSON error page Default value: NS_S_AS_ERROR_CODE_DESCRIPTION_DEFAULT

apispec Name of the API Specification. Default value: NS_S_APISPEC_DEFAULT

protoFileObject Name of the imported proto file. Default value: NS_S_AS_PROTOFILE_OBJECT_DEFAULT

JSONDoSAction One or more JSON Denial-of-Service (JsonDoS) actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -JSONDoSAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -JSONDoSAction none". Default value: AS_DEFAULT_DISPOSITION

JSONSQLInjectionAction One or more JSON SQL Injection actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -JSONSQLInjectionAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -JSONSQLInjectionAction none". Default value: AS_DEFAULT_DISPOSITION

JSONSQLInjectionType Available SQL injection types. -SQLSplChar : Checks for SQL Special Chars -SQLKeyword : Checks for SQL Keywords -SQLSplCharANDKeyword : Checks for both and blocks if both are found -SQLSplCharORKeyword : Checks for both and blocks if anyone is found, -None : Disables checking using both SQL Special Char and Keyword

Possible values: SQLSplChar, SQLKeyword, SQLSplCharORKeyword, SQLSplCharANDKeyword, None Default value: SQLSplCharANDKeyword

JSONSQLInjectionGrammar Check for SQL injection using SQL grammar in JSON

Possible values: ON, OFF Default value: OFF

JSONCMDInjectionAction One or more JSON CMD Injection actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -JSONCMDInjectionAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -JSONCMDInjectionAction none". Default value: AS_DEFAULT_DISPOSITION

JSONCMDInjectionType Available CMD injection types. -CMDSplChar : Checks for CMD Special Chars -CMDKeyword : Checks for CMD Keywords -CMDSplCharANDKeyword : Checks for both and blocks if both are found -CMDSplCharORKeyword : Checks for both and blocks if anyone is found, -None : Disables checking using both SQL Special Char and Keyword

Possible values: CMDSplChar, CMDKeyword, CMDSplCharORKeyword, CMDSplCharANDKeyword, None Default value: CMDSplCharANDKeyword

JSONCMDInjectionGrammar Check for CMD injection using CMD grammar in JSON

Possible values: ON, OFF Default value: OFF

JSONXSSAction One or more JSON Cross-Site Scripting actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -JSONXssAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -JSONXssAction none". Default value: AS_DEFAULT_DISPOSITION

XMLDoSAction One or more XML Denial-of-Service (XDoS) actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -XMLDoSAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLDoSAction none". Default value: AS_DEFAULT_DISPOSITION

XMLFormatAction One or more XML Format actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -XMLFormatAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLFormatAction none". Default value: AS_DEFAULT_DISPOSITION

XMLSQLInjectionAction One or more XML SQL Injection actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -XMLSQLInjectionAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLSQLInjectionAction none". Default value: AS_DEFAULT_DISPOSITION

XMLSQLInjectionType Available SQL injection types. -SQLSplChar : Checks for SQL Special Chars -SQLKeyword : Checks for SQL Keywords -SQLSplCharANDKeyword : Checks for both and blocks if both are found -SQLSplCharORKeyword : Checks for both and blocks if anyone is found

Possible values: SQLSplChar, SQLKeyword, SQLSplCharORKeyword, SQLSplCharANDKeyword, None

XMLSQLInjectionCheckSQLWildChars Check for form fields that contain SQL wild chars .

Possible values: ON, OFF

XMLSQLInjectionParseComments Parse comments in XML Data and exempt those sections of the request that are from the XML SQL Injection check. You must configure the type of comments that the application firewall is to detect and exempt from this security check. Available settings function as follows:

- Check all - Check all content.
- ANSI - Exempt content that is part of an ANSI (Mozilla-style) comment.
- Nested - Exempt content that is part of a nested (Microsoft-style) comment.
- ANSI Nested - Exempt content that is part of any type of comment.

Possible values: checkall, ansi, nested, ansinested Default value: checkall

XMLXSSAction One or more XML Cross-Site Scripting actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -XMLXSSAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLXSSAction none". Default value: AS_DEFAULT_DISPOSITION

XMLWSIAction One or more Web Services Interoperability (WSI) actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.

- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -XMLWSIAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLWSIAction none". Default value: AS_DEFAULT_DISPOSITION

XMLAttachmentAction One or more XML Attachment actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -XMLAttachmentAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLAttachmentAction none". Default value: AS_DEFAULT_DISPOSITION

XMLValidationAction One or more XML Validation actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -XMLValidationAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLValidationAction none". Default value: AS_DEFAULT_DISPOSITION

XMLErrorObject Name to assign to the XML Error Object, which the application firewall displays when a user request is blocked. Must begin with a letter, number, or the underscore character \(_\), and must contain only letters, numbers, and the hyphen \(-\), period \(.\) pound \(#\), space \(\), at (@), equals \(=\), colon \(:\), and underscore characters. Cannot be changed after the XML error object is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my XML error object" or 'my XML error object'\). Default value: NS_S_AS_ERROR_OBJECT_DEFAULT

XMLErrorStatusCode Response status code associated with XML error page. Non-empty XML error object must be imported to the application firewall profile for the status code. Default value: 200 Minimum value: 1 Maximum value: 999

XMLErrorStatusMessage Response status message associated with XML error page Default value: NS_S_AS_ERROR_CODE_DESCRIPTION_DEFAULT

signatures Object name for signatures. This check is applicable to Profile Type: HTML, XML. Default value: NS_S_AS_CUSTOM_OBJECT_DEFAULT

XMLSOAPFaultAction One or more XML SOAP Fault Filtering actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.
- Remove - Remove all violations for this security check.

CLI users: To enable one or more actions, type "set appfw profile -XMLSOAPFaultAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLSOAPFaultAction none". Default value: AS_DEFAULT_DISPOSITION

useHTMLErrorObject Send an imported HTML Error object to a user when a request is blocked, instead of redirecting the user to the designated Error URL.

Possible values: ON, OFF

errorURL URL that application firewall uses as the Error URL. Default value: NS_S_AS_ERROR_URL_DEFAULT

HTMLErrorObject Name to assign to the HTML Error Object. Must begin with a letter, number, or the underscore character \(_\), and must contain only letters, numbers, and the hyphen \(-\), period \(.\) pound \(#\), space \(\), at (@), equals \(=\), colon \(:\), and underscore characters. Cannot be changed after the HTML error object is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my HTML error object" or 'my HTML error object'\). Default value: NS_S_AS_ERROR_OBJECT_DEFAULT

HTMLErrorStatusCode Response status code associated with HTML error page. Non-empty HTML error object must be imported to the application firewall profile for the status code. Default value: 200 Minimum value: 1 Maximum value: 999

HTMLErrorStatusMessage Response status message associated with HTML error page Default value: NS_S_AS_ERROR_CODE_DESCRIPTION_DEFAULT

logEveryPolicyHit Log every profile match, regardless of security checks results.

Possible values: ON, OFF

stripHtmlComments Strip HTML comments before forwarding a web page sent by a protected web site in response to a user request.

Possible values: none, all, exclude_script_tag

stripXmlComments Strip XML comments before forwarding a web page sent by a protected web site in response to a user request.

Possible values: none, all

clientIpExpression Expression to get the client IP.

dynamicLearning One or more security checks. Available options are as follows:

- SQLInjection - Enable dynamic learning for SQLInjection security check.
- CrossSiteScripting - Enable dynamic learning for CrossSiteScripting security check.
- fieldFormat - Enable dynamic learning for fieldFormat security check.
- None - Disable security checks for all security checks.

CLI users: To enable dynamic learning on one or more security checks, type "set appfw profile -dynamicLearning" followed by the security checks to be enabled. To turn off dynamic learning on all security checks, type "set appfw profile -dynamicLearning none". Default value: AS_DYNAMIC_LEARNING_SECURITY_CHECK_DEFAULT

exemptClosureURLsFromSecurityChecks Exempt URLs that pass the Start URL closure check from SQL injection, cross-site script, field format and field consistency security checks at locations other than headers.

Possible values: ON, OFF

defaultCharSet Default character set for protected web pages. Web pages sent by your protected web sites in response to user requests are assigned this character set if the page does not already specify a character set. The character sets supported by the application firewall are:

- iso-8859-1 (English US)
- big5 (Chinese Traditional)
- gb2312 (Chinese Simplified)
- sjis (Japanese Shift-JIS)
- euc-jp (Japanese EUC-JP)
- iso-8859-9 (Turkish)
- utf-8 (Unicode)
- euc-kr (Korean) Default value: NS_S_AS_CHARSET_DEFAULT Maximum value: 31

postBodyLimit Maximum allowed HTTP post body size, in bytes. Maximum supported value is 10GB. Citrix recommends enabling streaming option for large values of post body limit (>20MB). Default value: 20000000 Minimum value: 0

postBodyLimitAction One or more Post Body Limit actions. Available settings function as follows:

- Block - Block connections that violate this security check. Must always be set.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.

CLI users: To enable one or more actions, type "set appfw profile -PostBodyLimitAction block" followed by the other actions to be enabled. Default value: AS_DEFAULT_POSTBODYLIMIT_DISPOSITION

postBodyLimitSignature Maximum allowed HTTP post body size for signature inspection for location HTTP_POST_BODY in the signatures, in bytes. Note that the changes in value could impact CPU and latency profile. Default value: 2048 Minimum value: 0

fileUploadMaxNum Maximum allowed number of file uploads per form-submission request. The maximum setting (65535) allows an unlimited number of uploads. Default value: 65535 Minimum value: 0 Maximum value: 65535

canonicalizeHTMLResponse Perform HTML entity encoding for any special characters in responses sent by your protected web sites.

Possible values: ON, OFF Default value: ON

enableFormTagging Enable tagging of web form fields for use by the Form Field Consistency and CSRF Form Tagging checks.

Possible values: ON, OFF Default value: ON

sessionlessFieldConsistency Perform sessionless Field Consistency Checks.

Possible values: OFF, ON, postOnly Default value: OFF

sessionlessURLClosure Enable session less URL Closure Checks. This check is applicable to Profile Type: HTML.

Possible values: ON, OFF Default value: OFF

semicolonFieldSeparator Allow ';' as a form field separator in URL queries and POST form bodies.

Possible values: ON, OFF Default value: OFF

excludeFileUploadFromChecks Exclude uploaded files from Form checks.

Possible values: ON, OFF Default value: OFF

SQLInjectionParseComments Parse HTML comments and exempt them from the HTML SQL Injection check. You must specify the type of comments that the application firewall is to detect and exempt from this security check. Available settings function as follows:

- Check all - Check all content.
- ANSI - Exempt content that is part of an ANSI (Mozilla-style) comment.
- Nested - Exempt content that is part of a nested (Microsoft-style) comment.
- ANSI Nested - Exempt content that is part of any type of comment.

Possible values: checkall, ansi, nested, ansinested Default value: AS_DEFAULT_SQLINJECTIONPARSECOMMENTS

invalidPercentHandling Configure the method that the application firewall uses to handle percent-encoded names and values. Available settings function as follows:

- asp_mode - Microsoft ASP format.
- secure_mode - Secure format.

Possible values: asp_mode, secure_mode Default value: secure_mode

type Application firewall profile type, which controls which security checks and settings are applied to content that is filtered with the profile. Available settings function as follows:

- HTML - HTML-based web sites.
- XML - XML-based web sites and services.
- JSON - JSON-based web sites and services.
- HTML XML (Web 2.0) - Sites that contain both HTML and XML content, such as ATOM feeds, blogs, and RSS feeds.
- HTML JSON - Sites that contain both HTML and JSON content.
- XML JSON - Sites that contain both XML and JSON content.
- HTML XML JSON - Sites that contain HTML, XML and JSON content. Default value: HTML

checkRequestHeaders Check request headers as well as web forms for injected SQL and cross-site scripts.

Possible values: ON, OFF Default value: OFF

inspectQueryContentTypes Inspect request query as well as web forms for injected SQL and cross-site scripts for following content types. Default value: AS_INSPECT_QUERY_DEFAULT

optimizePartialReqs Optimize handle of HTTP partial requests i.e. those with range headers. Available settings are as follows:

- ON - Partial requests by the client result in partial requests to the backend server in most cases.
- OFF - Partial requests by the client are changed to full requests to the backend server

Possible values: ON, OFF

URLDecodeRequestCookies URL Decode request cookies before subjecting them to SQL and cross-site scripting checks.

Possible values: ON, OFF Default value: OFF

comment Any comments about the purpose of profile, or other useful information about the profile.

percentDecodeRecursively Configure whether the application firewall should use percentage recursive decoding

Possible values: ON, OFF Default value: ON

multipleHeaderAction One or more multiple header actions. Available settings function as follows:

- Block - Block connections that have multiple headers.
- Log - Log connections that have multiple headers.
- KeepLast - Keep only last header when multiple headers are present.

Request headers inspected:

- Accept-Encoding
- Content-Encoding
- Content-Range
- Content-Type
- Host
- Range
- Referer

CLI users: To enable one or more actions, type "set appfw profile -multipleHeaderAction" followed by the actions to be enabled. Default value: AS_MULTIPLE_HEADER_DEFAULT_DISPOSITION

rfcprofile Object name of the rfc profile. Default value: NS_S_AS_RFC_PROFILE_DEFAULT

fileUploadTypesAction One or more file upload types actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -fileUploadTypeAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -fileUploadTypeAction none". Default value: AS_DEFAULT_DISPOSITION

verboseLogLevel Detailed Logging Verbose Log Level.

Possible values: pattern, patternPayload, patternPayloadHeader Default value: pattern

insertCookieSameSiteAttribute Configure whether application firewall should add samesite attribute for set-cookies

Possible values: ON, OFF Default value: OFF

cookieSameSiteAttribute Cookie Samesite attribute added to support adding cookie SameSite attribute for all set-cookies including appfw session cookies. Default value will be "SameSite=Lax".

Possible values: None, LAX, STRICT Default value: LAX

SQLInjectionRuleType Specifies SQL Injection rule type: ALLOW/DENY. If ALLOW rule type is configured then allow list rules are used, if DENY rule type is configured then deny rules are used.

Possible values: ALLOW, DENY Default value: ALLOW

FakeAccountDetection Fake account detection flag : ON/OFF. If set to ON fake account detection in enabled on ADC, if set to OFF fake account detection is disabled.

Possible values: ON, OFF Default value: OFF

GeoLocationLogging Enable Geo-Location Logging in CEF format logs for the profile.

Possible values: ON, OFF

CEFlogging Enable CEF format logs for the profile.

Possible values: ON, OFF

blockKeywordAction Block Keyword action. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -blockKeywordAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -blockKeywordAction none". Default value: none

JSONBlockKeywordAction JSON Block Keyword action. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.

- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -JSONBlockKeywordAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -JSONBlockKeywordAction none". Default value: none

bypasslist Enable bypass list for the profile.

Possible values: ON, OFF Default value: OFF

denylist Enable deny list for the profile.

Possible values: ON, OFF Default value: OFF

sessionCookieName Name of the session cookie that the application firewall uses to track user sessions. Must begin with a letter or number, and can consist of from 1 to 31 letters, numbers, and the hyphen (-) and underscore (_) symbols.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cookie name" or 'my cookie name').

restore appfw profile

Restore configuration from archive file

Synopsis

restore appfw profile <archivename>

Arguments

archivename Source for tar archive.

relaxationRules Import all appfw relaxation rules

importProfileName Name of the profile which will be created/updated to associate the relaxation rules

matchUrlString Match this action url in archived Relaxation Rules to replace.

replaceUrlString Replace matched url string with this action url string while restoring Relaxation Rules

overwrite Purge existing Relaxation Rules and replace during import

augment Augment Relaxation Rules during import

Related Commands

- import appfw archive

add appfw profile

Creates an application firewall profile, which specifies how the application firewall should protect a given type of web content. (A profile is equivalent to an action in other Citrix ADC features.)

Synopsis

add appfw profile <name>

Arguments

name Name for the profile. Must begin with a letter, number, or the underscore character (*), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at (@), equals (=), colon (:), and underscore (*) characters. Cannot be changed after the profile is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

defaults Default configuration to apply to the profile. Basic defaults are intended for standard content that requires little further configuration, such as static web site content. Advanced defaults are intended for specialized content that requires significant specialized configuration, such as heavily scripted or dynamic content.

CLI users: When adding an application firewall profile, you can set either the defaults or the type, but not both. To set both options, create the profile by using the add appfw profile command, and then use the set appfw profile command to configure the other option.

Possible values: basic, advanced, core, cve

startURLAction One or more Start URL actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.
- Log - Log violations of this security check.

- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -startURLaction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -startURLaction none". Default value: AS_DEFAULT_DISPOSITION

inferContentTypeXmlPayloadAction One or more infer content type payload actions. Available settings function as follows:

- Block - Block connections that have mismatch in content-type header and payload.
- Log - Log connections that have mismatch in content-type header and payload. The mismatched content-type in HTTP request header will be logged for the request.
- Stats - Generate statistics when there is mismatch in content-type header and payload.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -inferContentTypeXMLPayloadAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -inferContentTypeXMLPayloadAction none". Please note "none" action cannot be used with any other action type. Default value: AS_INFER_CONTENT_TYPE_XML_PAYLOAD_DEFAULT_DISPOSITION

contentTypeAction One or more Content-type actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -contentTypeaction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -contentTypeaction none". Default value: AS_DEFAULT_CONTENT_TYPE_DISPOSITION

inspectContentTypes One or more InspectContentType lists.

- application/x-www-form-urlencoded
- multipart/form-data
- text/x-gwt-rpc

CLI users: To enable, type "set appfw profile -InspectContentTypes" followed by the content types to be inspected. Default value: AS_DEFAULT_INSPECTION_CONTENT_TYPE

startURLClosure Toggle the state of Start URL Closure.

Possible values: ON, OFF Default value: OFF

denyURLAction One or more Deny URL actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

NOTE: The Deny URL check takes precedence over the Start URL check. If you enable blocking for the Deny URL check, the application firewall blocks any URL that is explicitly blocked by a Deny URL, even if the same URL would otherwise be allowed by the Start URL check.

CLI users: To enable one or more actions, type "set appfw profile -denyURLaction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -denyURLaction none". Default value: AS_DEFAULT_DISPOSITION

RefererHeaderCheck Enable validation of Referer headers. Referer validation ensures that a web form that a user sends to your web site originally came from your web site, not an outside attacker. Although this parameter is part of the Start URL check, referer validation protects against cross-site request forgery (CSRF) attacks, not Start URL attacks.

Possible values: OFF, if_present, AlwaysExceptStartURLs, AlwaysExceptFirstRequest Default value: OFF

cookieConsistencyAction One or more Cookie Consistency actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -cookieConsistencyAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -cookieConsistencyAction none". Default value: none

cookieHijackingAction One or more actions to prevent cookie hijacking. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check. NOTE: Cookie Hijacking feature is not supported for TLSv1.3

CLI users: To enable one or more actions, type "set appfw profile -cookieHijackingAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -cookieHijackingAction none". Default value: none

cookieTransforms Perform the specified type of cookie transformation. Available settings function as follows:

- Encryption - Encrypt cookies.
- Proxying - Mask contents of server cookies by sending proxy cookie to users.
- Cookie flags - Flag cookies as HTTP only to prevent scripts on user's browser from accessing and possibly modifying them. CAUTION: Make sure that this parameter is set to ON if you are configuring any cookie transformations. If it is set to OFF, no cookie transformations are performed regardless of any other settings.

Possible values: ON, OFF Default value: OFF

cookieEncryption Type of cookie encryption. Available settings function as follows:

- None - Do not encrypt cookies.
- Decrypt Only - Decrypt encrypted cookies, but do not encrypt cookies.
- Encrypt Session Only - Encrypt session cookies, but not permanent cookies.
- Encrypt All - Encrypt all cookies.

Possible values: none, decryptOnly, encryptSessionOnly, encryptAll Default value: none

cookieProxying Cookie proxy setting. Available settings function as follows:

- None - Do not proxy cookies.
- Session Only - Proxy session cookies by using the Citrix ADC session ID, but do not proxy permanent cookies.

Possible values: none, sessionOnly Default value: none

addCookieFlags Add the specified flags to cookies. Available settings function as follows:

- None - Do not add flags to cookies.
- HTTP Only - Add the HTTP Only flag to cookies, which prevents scripts from accessing cookies.
- Secure - Add Secure flag to cookies.
- All - Add both HTTPOnly and Secure flags to cookies.

Possible values: none, httpOnly, secure, all Default value: none

fieldConsistencyAction One or more Form Field Consistency actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -fieldConsistencyaction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -fieldConsistencyAction none". Default value: none

CSRFtagAction One or more Cross-Site Request Forgery (CSRF) Tagging actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -CSRFTagAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -CSRFTagAction none". Default value: none

crossSiteScriptingAction One or more Cross-Site Scripting (XSS) actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -crossSiteScriptingAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -crossSiteScriptingAction none". Default value: AS_DEFAULT_DISPOSITION

crossSiteScriptingTransformUnsafeHTML Transform cross-site scripts. This setting configures the application firewall to disable dangerous HTML instead of blocking the request. CAUTION: Make sure that this parameter is set to ON if you are configuring any cross-site scripting transformations. If it is set to OFF, no cross-site scripting transformations are performed regardless of any other settings.

Possible values: ON, OFF Default value: OFF

crossSiteScriptingCheckCompleteURLs Check complete URLs for cross-site scripts, instead of just the query portions of URLs.

Possible values: ON, OFF Default value: OFF

SQLInjectionAction One or more HTML SQL Injection actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -SQLInjectionAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -SQLInjectionAction none". Default value: AS_DEFAULT_DISPOSITION

CMDInjectionAction Command injection action. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -cmdInjectionAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -cmdInjectionAction none". Default value: none

CMDInjectionType Available CMD injection types. -CMDSplChar : Checks for CMD Special Chars -CMDKeyword : Checks for CMD Keywords -CMDSplCharANDKeyword : Checks for both and blocks if both are found -CMDSplCharORKeyword : Checks for both and blocks if anyone is found, -None : Disables checking using both CMD Special Char and Keyword

Possible values: CMDSplChar, CMDKeyword, CMDSplCharORKeyword, CMDSplCharANDKeyword, None Default value: CMDSplCharANDKeyword

SQLInjectionGrammar Check for SQL injection using SQL grammar

Possible values: ON, OFF Default value: OFF

CMDInjectionGrammar Check for CMD injection using CMD grammar

Possible values: ON, OFF Default value: OFF

SQLInjectionTransformSpecialChars Transform injected SQL code. This setting configures the application firewall to disable SQL special strings instead of blocking the request. Since most SQL servers require a special string to activate an SQL keyword, in most cases a request that contains injected SQL code is safe if special strings are disabled. CAUTION: Make sure that this parameter is set to ON if you are configuring any SQL injection transformations. If it is set to OFF, no SQL injection transformations are performed regardless of any other settings.

Possible values: ON, OFF Default value: OFF

SQLInjectionType Available SQL injection types. -SQLSplChar : Checks for SQL Special Chars -SQLKeyword : Checks for SQL Keywords -SQLSplCharANDKeyword : Checks for both and blocks if both are found -SQLSplCharORKeyword : Checks for both and blocks if anyone is found -None : Disables checking using both SQL Special Char and Keyword

Possible values: SQLSplChar, SQLKeyword, SQLSplCharORKeyword, SQLSplCharANDKeyword, None Default value: SQLSplCharANDKeyword

SQLInjectionCheckSQLWildChars Check for form fields that contain SQL wild chars .

Possible values: ON, OFF Default value: OFF

fieldFormatAction One or more Field Format actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of suggested web form fields and field format assignments.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -fieldFormatAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -fieldFormatAction none". Default value: AS_DEFAULT_DISPOSITION

defaultFieldFormatType Designate a default field type to be applied to web form fields that do not have a field type explicitly assigned to them.

defaultFieldFormatMinLength Minimum length, in characters, for data entered into a field that is assigned the default field type. To disable the minimum and maximum length settings and allow data of any length to be entered into the field, set this parameter to zero (0). Default value: 0 Minimum value: 0 Maximum value: 2147483647

defaultFieldFormatMaxLength Maximum length, in characters, for data entered into a field that is assigned the default field type. Default value: 65535 Minimum value: 1 Maximum value: 2147483647

bufferOverflowAction One or more Buffer Overflow actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.

- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -bufferOverflowAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -bufferOverflowAction none". Default value: AS_DEFAULT_DISPOSITION

grpcAction gRPC validation Default value: AS_DEFAULT_GRPC_DISPOSITION

restAction rest validation Default value: AS_DEFAULT_GRPC_DISPOSITION

bufferOverflowMaxURLLength Maximum length, in characters, for URLs on your protected web sites. Requests with longer URLs are blocked. Default value: 1024 Minimum value: 0 Maximum value: 65535

bufferOverflowMaxHeaderLength Maximum length, in characters, for HTTP headers in requests sent to your protected web sites. Requests with longer headers are blocked. Default value: 4096 Minimum value: 0 Maximum value: 65535

bufferOverflowMaxCookieLength Maximum length, in characters, for cookies sent to your protected web sites. Requests with longer cookies are blocked. Default value: 4096 Minimum value: 0 Maximum value: 65535

bufferOverflowMaxQueryLength Maximum length, in bytes, for query string sent to your protected web sites. Requests with longer query strings are blocked. Default value: 65535 Minimum value: 0 Maximum value: 65535

bufferOverflowMaxTotalHeaderLength Maximum length, in bytes, for the total HTTP header length in requests sent to your protected web sites. The minimum value of this and maxHeaderLen in httpProfile will be used. Requests with longer length are blocked. Default value: 65535 Minimum value: 0 Maximum value: 65535

creditCardAction One or more Credit Card actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -creditCardAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -creditCardAction none". Default value: none

creditCard Credit card types that the application firewall should protect. Default value: none

creditCardMaxAllowed This parameter value is used by the block action. It represents the maximum number of credit card numbers that can appear on a web page served by your protected web sites. Pages that contain more credit card numbers are blocked. Minimum value: 0 Maximum value: 255

creditCardXOut Mask any credit card number detected in a response by replacing each digit, except the digits in the final group, with the letter "X."

Possible values: ON, OFF Default value: OFF

doSecureCreditCardLogging Setting this option logs credit card numbers in the response when the match is found.

Possible values: ON, OFF Default value: ON

streaming Setting this option converts content-length form submission requests (requests with content-type "application/x-www-form-urlencoded" or "multipart/form-data") to chunked requests when atleast one of the following protections : Signatures, SQL injection protection, XSS protection, form field consistency protection, starturl closure, CSRF tagging, JSON SQL, JSON XSS, JSON DOS is enabled. Please make sure that the backend server accepts chunked requests before enabling this option. Citrix recommends enabling this option for large request sizes(>20MB).

Possible values: ON, OFF Default value: OFF

trace Toggle the state of trace

Possible values: ON, OFF Default value: OFF

requestContentType Default Content-Type header for requests. A Content-Type header can contain 0-255 letters, numbers, and the hyphen (-) and underscore (_) characters. Default value: NS_S_AS_DEFAULT_REQUEST_CONTENT_TYPE

responseContentType Default Content-Type header for responses. A Content-Type header can contain 0-255 letters, numbers, and the hyphen (-) and underscore (_) characters. Default value: NS_S_AS_DEFAULT_RESPONSE_CONTENT_TYPE

JSONErrorObject Name to the imported JSON Error Object to be set on application firewall profile.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my JSON error object" or 'my JSON error object'\). Default value: NS_S_AS_ERROR_OBJECT_DEFAULT

apispec Name of the API Specification. Default value: NS_S_APISPEC_DEFAULT

protoFileObject Name of the imported proto file. Default value: NS_S_AS_PROTOFILE_OBJECT_DEFAULT

JSONErrorStatusCode Response status code associated with JSON error page. Non-empty JSON error object must be imported to the application firewall profile for the status code. Default value: 200 Minimum value: 1 Maximum value: 999

JSONErrorStatusMessage Response status message associated with JSON error page Default value: NS_S_AS_ERROR_CODE_DESCRIPTION_DEFAULT

JSONDoSAction One or more JSON Denial-of-Service (JsonDoS) actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -JSONDoSAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -JSONDoSAction none". Default value: AS_DEFAULT_DISPOSITION

JSONSQLInjectionAction One or more JSON SQL Injection actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -JSONSQLInjectionAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -JSONSQLInjectionAction none". Default value: AS_DEFAULT_DISPOSITION

JSONSQLInjectionType Available SQL injection types. -SQLSplChar : Checks for SQL Special Chars -SQLKeyword : Checks for SQL Keywords -SQLSplCharANDKeyword : Checks for both and blocks if both are found -SQLSplCharORKeyword : Checks for both and blocks if anyone is found, -None : Disables checking using both SQL Special Char and Keyword

Possible values: SQLSplChar, SQLKeyword, SQLSplCharORKeyword, SQLSplCharANDKeyword, None Default value: SQLSplCharANDKeyword

JSONSQLInjectionGrammar Check for SQL injection using SQL grammar in JSON

Possible values: ON, OFF Default value: OFF

JSONCMDInjectionAction One or more JSON CMD Injection actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -JSONCMDInjectionAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -JSONCMDInjectionAction none". Default value: AS_DEFAULT_DISPOSITION

JSONCMDInjectionType Available CMD injection types. -CMDSplChar : Checks for CMD Special Chars -CMDKeyword : Checks for CMD Keywords -CMDSplCharANDKeyword : Checks for both and blocks if both are found -CMDSplCharORKeyword : Checks for both and blocks if anyone is found, -None : Disables checking using both SQL Special Char and Keyword

Possible values: CMDSplChar, CMDKeyword, CMDSplCharORKeyword, CMDSplCharANDKeyword, None Default value: CMDSplCharANDKeyword

JSONCMDInjectionGrammar Check for CMD injection using CMD grammar in JSON

Possible values: ON, OFF Default value: OFF

JSONXSSAction One or more JSON Cross-Site Scripting actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -JSONXssAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -JSONXssAction none". Default value: AS_DEFAULT_DISPOSITION

XMLDoSAction One or more XML Denial-of-Service (XDoS) actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -XMLDoSAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLDoSAction none". Default value: AS_DEFAULT_DISPOSITION

XMLFormatAction One or more XML Format actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -XMLFormatAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLFormatAction none". Default value: AS_DEFAULT_DISPOSITION

XMLSQLInjectionAction One or more XML SQL Injection actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.

- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -XMLSQLInjectionAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLSQLInjectionAction none". Default value: AS_DEFAULT_DISPOSITION

XMLSQLInjectionType Available SQL injection types. -SQLSplChar : Checks for SQL Special Chars -SQLKeyword : Checks for SQL Keywords -SQLSplCharANDKeyword : Checks for both and blocks if both are found -SQLSplCharORKeyword : Checks for both and blocks if anyone is found

Possible values: SQLSplChar, SQLKeyword, SQLSplCharORKeyword, SQLSplCharANDKeyword, None Default value: SQLSplCharANDKeyword

XMLSQLInjectionCheckSQLWildChars Check for form fields that contain SQL wild chars .

Possible values: ON, OFF Default value: OFF

XMLSQLInjectionParseComments Parse comments in XML Data and exempt those sections of the request that are from the XML SQL Injection check. You must configure the type of comments that the application firewall is to detect and exempt from this security check. Available settings function as follows:

- Check all - Check all content.
- ANSI - Exempt content that is part of an ANSI (Mozilla-style) comment.
- Nested - Exempt content that is part of a nested (Microsoft-style) comment.
- ANSI Nested - Exempt content that is part of any type of comment.

Possible values: checkall, ansi, nested, ansinested Default value: checkall

XMLXSSAction One or more XML Cross-Site Scripting actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -XMLXSSAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLXSSAction none". Default value: AS_DEFAULT_DISPOSITION

XMLWSIAction One or more Web Services Interoperability (WSI) actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -XMLWSIAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLWSIAction none". Default value: AS_DEFAULT_DISPOSITION

XMLAttachmentAction One or more XML Attachment actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Learn - Use the learning engine to generate a list of exceptions to this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -XMLAttachmentAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLAttachmentAction none". Default value: AS_DEFAULT_DISPOSITION

XMLValidationAction One or more XML Validation actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -XMLValidationAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLValidationAction none". Default value: AS_DEFAULT_DISPOSITION

XMLErrorObject Name to assign to the XML Error Object, which the application firewall displays when a user request is blocked. Must begin with a letter, number, or the underscore character \(_\), and must contain only letters, numbers, and the hyphen \(-\), period \(.\) pound \(#\), space \(\), at (@), equals \(=\), colon \(:\), and underscore characters. Cannot be changed after the XML error object is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my XML error object" or 'my XML error object'\). Default value: NS_S_AS_ERROR_OBJECT_DEFAULT

XMLErrorStatusCode Response status code associated with XML error page. Non-empty XML error object must be imported to the application firewall profile for the status code. Default value: 200 Minimum value: 1 Maximum value: 999

XMLErrorStatusMessage Response status message associated with XML error page Default value: NS_S_AS_ERROR_CODE_DESCRIPTION_DEFAULT

signatures Object name for signatures. This check is applicable to Profile Type: HTML, XML. Default value: NS_S_AS_CUSTOM_OBJECT_DEFAULT

XMLSOAPFaultAction One or more XML SOAP Fault Filtering actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.
- Remove - Remove all violations for this security check.

CLI users: To enable one or more actions, type "set appfw profile -XMLSOAPFaultAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLSOAPFaultAction none". Default value: AS_DEFAULT_DISPOSITION

useHTMLErrorObject Send an imported HTML Error object to a user when a request is blocked, instead of redirecting the user to the designated Error URL.

Possible values: ON, OFF Default value: OFF

errorURL URL that application firewall uses as the Error URL. Default value: NS_S_AS_ERROR_URL_DEFAULT

HTMLErrorObject Name to assign to the HTML Error Object. Must begin with a letter, number, or the underscore character \(_\), and must contain only letters, numbers, and the hyphen \(-\), period \(.\) pound \(#\), space \(\), at (@), equals \(=\), colon \(:\), and underscore characters. Cannot be changed after the HTML error object is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my HTML error object" or 'my HTML error object'\). Default value: NS_S_AS_ERROR_OBJECT_DEFAULT

HTMLErrorStatusCode Response status code associated with HTML error page. Non-empty HTML error object must be imported to the application firewall profile for the status code. Default value: 200 Minimum value: 1 Maximum value: 999

HTMLErrorStatusMessage Response status message associated with HTML error page Default value: NS_S_AS_ERROR_CODE_DESCRIPTION_DEFAULT

logEveryPolicyHit Log every profile match, regardless of security checks results.

Possible values: ON, OFF Default value: OFF

stripHtmlComments Strip HTML comments before forwarding a web page sent by a protected web site in response to a user request.

Possible values: none, all, exclude_script_tag Default value: none

stripXmlComments Strip XML comments before forwarding a web page sent by a protected web site in response to a user request.

Possible values: none, all Default value: none

exemptClosureURLsFromSecurityChecks Exempt URLs that pass the Start URL closure check from SQL injection, cross-site script, field format and field consistency security checks at locations other than headers.

Possible values: ON, OFF Default value: ON

defaultCharSet Default character set for protected web pages. Web pages sent by your protected web sites in response to user requests are assigned this character set if the page does not already specify a character set. The character sets supported by the application firewall are:

- iso-8859-1 (English US)
- big5 (Chinese Traditional)
- gb2312 (Chinese Simplified)
- sjis (Japanese Shift-JIS)
- euc-jp (Japanese EUC-JP)
- iso-8859-9 (Turkish)
- utf-8 (Unicode)
- euc-kr (Korean) Default value: NS_S_AS_CHARSET_DEFAULT Maximum value: 31

clientIpExpression Expression to get the client IP.

dynamicLearning One or more security checks. Available options are as follows:

- SQLInjection - Enable dynamic learning for SQLInjection security check.
- CrossSiteScripting - Enable dynamic learning for CrossSiteScripting security check.
- fieldFormat - Enable dynamic learning for fieldFormat security check.
- None - Disable security checks for all security checks.

CLI users: To enable dynamic learning on one or more security checks, type "set appfw profile -dynamicLearning" followed by the security checks to be enabled. To turn off dynamic learning on all security checks, type "set appfw profile -dynamicLearning none". Default value: AS_DYNAMIC_LEARNING_SECURITY_CHECK_DEFAULT

postBodyLimit Maximum allowed HTTP post body size, in bytes. Maximum supported value is 10GB. Citrix recommends enabling streaming option for large values of post body limit (>20MB). Default value: 20000000 Minimum value: 0

postBodyLimitAction One or more Post Body Limit actions. Available settings function as follows:

- Block - Block connections that violate this security check. Must always be set.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.

CLI users: To enable one or more actions, type "set appfw profile -PostBodyLimitAction block" followed by the other actions to be enabled. Default value: AS_DEFAULT_POSTBODYLIMIT_DISPOSITION

postBodyLimitSignature Maximum allowed HTTP post body size for signature inspection for location HTTP_POST_BODY in the signatures, in bytes. Note that the changes in value could impact CPU and latency profile. Default value: 2048 Minimum value: 0

fileUploadMaxNum Maximum allowed number of file uploads per form-submission request. The maximum setting (65535) allows an unlimited number of uploads. Default value: 65535 Minimum value: 0 Maximum value: 65535

canonicalizeHTMLResponse Perform HTML entity encoding for any special characters in responses sent by your protected web sites.

Possible values: ON, OFF Default value: ON

enableFormTagging Enable tagging of web form fields for use by the Form Field Consistency and CSRF Form Tagging checks.

Possible values: ON, OFF Default value: ON

sessionlessFieldConsistency Perform sessionless Field Consistency Checks.

Possible values: OFF, ON, postOnly Default value: OFF

sessionlessURLClosure Enable session less URL Closure Checks. This check is applicable to Profile Type: HTML.

Possible values: ON, OFF Default value: OFF

semicolonFieldSeparator Allow ';' as a form field separator in URL queries and POST form bodies.

Possible values: ON, OFF Default value: OFF

excludeFileUploadFromChecks Exclude uploaded files from Form checks.

Possible values: ON, OFF Default value: OFF

SQLInjectionParseComments Parse HTML comments and exempt them from the HTML SQL Injection check. You must specify the type of comments that the application firewall is to detect and exempt from this security check. Available settings function as follows:

- Check all - Check all content.
- ANSI - Exempt content that is part of an ANSI (Mozilla-style) comment.
- Nested - Exempt content that is part of a nested (Microsoft-style) comment.

- ANSI Nested - Exempt content that is part of any type of comment.

Possible values: checkall, ansi, nested, ansinested Default value: AS_DEFAULT_SQLINJECTIONPARSECOMMENTS

invalidPercentHandling Configure the method that the application firewall uses to handle percent-encoded names and values. Available settings function as follows:

- asp_mode - Microsoft ASP format.
- secure_mode - Secure format.

Possible values: asp_mode, secure_mode Default value: secure_mode

type Application firewall profile type, which controls which security checks and settings are applied to content that is filtered with the profile. Available settings function as follows:

- HTML - HTML-based web sites.
- XML - XML-based web sites and services.
- JSON - JSON-based web sites and services.
- HTML XML (Web 2.0) - Sites that contain both HTML and XML content, such as ATOM feeds, blogs, and RSS feeds.
- HTML JSON - Sites that contain both HTML and JSON content.
- XML JSON - Sites that contain both XML and JSON content.
- HTML XML JSON - Sites that contain HTML, XML and JSON content. Default value: HTML

checkRequestHeaders Check request headers as well as web forms for injected SQL and cross-site scripts.

Possible values: ON, OFF Default value: OFF

inspectQueryContentTypes Inspect request query as well as web forms for injected SQL and cross-site scripts for following content types. Default value: AS_INSPECT_QUERY_DEFAULT

optimizePartialReqs Optimize handle of HTTP partial requests i.e. those with range headers. Available settings are as follows:

- ON - Partial requests by the client result in partial requests to the backend server in most cases.
- OFF - Partial requests by the client are changed to full requests to the backend server

Possible values: ON, OFF Default value: ON

URLDecodeRequestCookies URL Decode request cookies before subjecting them to SQL and cross-site scripting checks.

Possible values: ON, OFF Default value: OFF

comment Any comments about the purpose of profile, or other useful information about the profile.

percentDecodeRecursively Configure whether the application firewall should use percentage recursive decoding

Possible values: ON, OFF Default value: ON

multipleHeaderAction One or more multiple header actions. Available settings function as follows:

- Block - Block connections that have multiple headers.
- Log - Log connections that have multiple headers.
- KeepLast - Keep only last header when multiple headers are present.

Request headers inspected:

- Accept-Encoding
- Content-Encoding
- Content-Range
- Content-Type
- Host
- Range
- Referer

CLI users: To enable one or more actions, type "set appfw profile -multipleHeaderAction" followed by the actions to be enabled. Default value: AS_MULTIPLE_HEADER_DEFAULT_DISPOSITION

rfcprofile Object name of the rfc profile. Default value: NS_S_AS_RFC_PROFILE_DEFAULT

fileUploadTypesAction One or more file upload types actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -fileUploadTypeAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -fileUploadTypeAction none". Default value: AS_DEFAULT_DISPOSITION

verboseLogLevel Detailed Logging Verbose Log Level.

Possible values: pattern, patternPayload, patternPayloadHeader Default value: pattern

insertCookieSameSiteAttribute Configure whether application firewall should add samesite attribute for set-cookies

Possible values: ON, OFF Default value: OFF

cookieSameSiteAttribute Cookie Samesite attribute added to support adding cookie SameSite attribute for all set-cookies including appfw session cookies. Default value will be "SameSite=Lax".

Possible values: None, LAX, STRICT Default value: LAX

SQLInjectionRuleType Specifies SQL Injection rule type: ALLOW/DENY. If ALLOW rule type is configured then allow list rules are used, if DENY rule type is configured then deny rules are used.

Possible values: ALLOW, DENY Default value: ALLOW

FakeAccountDetection Fake account detection flag : ON/OFF. If set to ON fake account detection in enabled on ADC, if set to OFF fake account detection is disabled.

Possible values: ON, OFF Default value: OFF

GeoLocationLogging Enable Geo-Location Logging in CEF format logs for the profile.

Possible values: ON, OFF

CEFlogging Enable CEF format logs for the profile.

Possible values: ON, OFF

blockKeywordAction Block Keyword action. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -blockKeywordAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -blockKeywordAction none". Default value: none

JSONBlockKeywordAction JSON Block Keyword action. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -JSONBlockKeywordAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -JSONBlockKeywordAction none". Default value: none

bypasslist Enable bypass list for the profile.

Possible values: ON, OFF Default value: OFF

denylist Enable deny list for the profile.

Possible values: ON, OFF Default value: OFF

sessionCookieName Name of the session cookie that the application firewall uses to track user sessions. Must begin with a letter or number, and can consist of from 1 to 31 letters, numbers, and the hyphen (-) and underscore (_) symbols.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cookie name" or 'my cookie name').

archive appfw profile

Create archive for the profile.

Synopsis

archive appfw profile <name> <archivename>

Arguments

name Name for the profile. Must begin with a letter, number, or the underscore character (*), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at (@), equals (=), colon (:), and underscore (*) characters. Cannot be changed after the profile is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

archivename Source for tar archive.

comment Any comments about the purpose of profile, or other useful information about the profile.

Related Commands

- import appfw archive

rm appfw profile

Removes the specified application firewall profile.

Synopsis

rm appfw profile <name>

Arguments

name Name of the profile.

show appfw profile

Displays details of the specified application firewall profile. If no profile is specified, displays a list of all application firewall profiles on the Citrix ADC.

Synopsis

show appfw profile

Arguments

name Name of the application firewall profile.

Output

stateflag type The profile type of of this Application Firewall profile. If the profile is of the HTML type, only checks relevant to HTML are applied. If the profile is of the XML type, only checks relevent to XML are applied. if the profile is of the Web 2.0 type, then both types of checks are applied.

state Enabled.

defaults Default configuration to apply to the profile. Basic defaults are intended for standard content that requires little further configuration, such as static web site content. Advanced defaults are intended for specialized content that requires significant specialized configuration, such as heavily scripted or dynamic content.

CLI users: When adding an application firewall profile, you can set either the defaults or the type, but not both. To set both options, create the profile by using the add appfw profile command, and then use the set appfw profile command to configure the other option.

useHTMLErrorObject Send an imported HTML Error object to a user when a request is blocked, instead of redirecting the user to the designated Error URL.

errorURL The error page for this profile.

HTMLErrorObject Name to assign to the HTML Error Object. Must begin with a letter, number, or the underscore character \(_\), and must contain only letters, numbers, and the hyphen \(-\), period \(.\) pound \(#\), space \(\), at (@), equals \(=\), colon \(:\), and underscore characters. Cannot be changed after the HTML error object is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my HTML error object" or 'my HTML error object'\).

HTMLErrorStatusCode Response status code associated with HTML error page. Non-empty HTML error object must be imported to the application firewall profile for the status code.

HTMLErrorStatusMessage Response status message associated with HTML error page

logEveryPolicyHit Log every profile match, regardless of security checks results.

stripComments Tells the Application Firewall to strip HTML comments from responses before sending them to the user.

stripHtmlComments Tells the Application Firewall to strip HTML comments from responses before sending them to the user.

stripXmlComments Tells the Application Firewall to strip XML comments from responses before sending them to the user.

defaultCharSet The default character set. The character set that the Application Firewall uses for web pages that do not explicitly set a different character set.

postBodyLimit The maximum body size for an HTTP POST.

postBodyLimitAction One or more Post Body Limit actions. Available settings function as follows:

- Block - Block connections that violate this security check. Must always be set.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.

CLI users: To enable one or more actions, type "set appfw profile -PostBodyLimitAction block" followed by the other actions to be enabled.

clientIpExpression Expression to get the client IP.

dynamicLearning One or more security checks. Available options are as follows:

- SQLInjection - Enable dynamic learning for SQLInjection security check.
- CrossSiteScripting - Enable dynamic learning for CrossSiteScripting security check.
- fieldFormat - Enable dynamic learning for fieldFormat security check.
- None - Disable security checks for all security checks.

CLI users: To enable dynamic learning on one or more security checks, type "set appfw profile -dynamicLearning" followed by the security checks to be enabled. To turn off dynamic learning on all security checks, type "set appfw profile -dynamicLearning none".

isAutoDeployed Is the rule auto deployed by dynamic profile ?

alertOnly Send SNMP alert?

postBodyLimitSignature Maximum allowed HTTP post body size for signature inspection for location HTTP_POST_BODY in the signatures, in bytes. Note that the changes in value could impact CPU and latency profile.

learning Profile level learning option that overrides the protection level learning. Available settings are as follows:

- ON - Honor all protection level learn settings.
- OFF - Avoids learning for this profile for all protections ignoring protection level learn setting.

fileUploadMaxNum Maximum allowed number of file uploads per form-submission request. The maximum setting (65535) allows an unlimited number of uploads.

canonicalizeHTMLResponse Tells the Application Firewall to convert any non-ASCII characters into HTML entities before sending responses to the user. This is called 'canonicalization' of HTML responses.

enableFormTagging Enables tagging of web forms for form field Consistency checks.

sessionlessFieldConsistency Enable session less form field consistency checks.

sessionlessURLClosure Enable session less URL closure checks.

semicolonFieldSeparator Allow ';' as a form field separator in URL queries and POST form bodies.

excludeFileUploadFromChecks Excludes uploaded files from all web form checks.

SQLInjectionParseComments Canonicalizes SQL Comments in form fields.

checkRequestHeaders Check request headers as well as web forms for injected SQL and cross-site scripts.

inspectQueryContentTypes Inspect request query as well as web forms for injected SQL and cross-site scripts for following content types.

optimizePartialReqs Optimize handle of HTTP partial requests i.e. those with range headers. Available settings are as follows:

- ON - Partial requests by the client result in partial requests to the backend server in most cases.
- OFF - Partial requests by the client are changed to full requests to the backend server

URLDecodeRequestCookies URL Decode request cookies before subjecting them to SQL and cross-site scripting checks.

startURLAction Start URL action types. (BLOCK | LEARN | LOG | STATS | NONE)

inferContentTypeXmlPayloadAction One or more infer content type payload actions. Available settings function as follows:

- Block - Block connections that have mismatch in content-type header and payload.
- Log - Log connections that have mismatch in content-type header and payload. The mismatched content-type in HTTP request header will be logged for the request.
- Stats - Generate statistics when there is mismatch in content-type header and payload.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -inferContentTypeXMLPayloadAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -inferContentTypeXMLPayloadAction none". Please note "none" action cannot be used with any other action type.

contentTypeAction Content-type action types. (BLOCK | LOG | NONE)

inspectContentTypes Inspection content types associated with this profile

startURL A regular expression that designates a URL on the Start URL list.

startURLClosure Enable Start URL closure. When enabled, this feature allows users to start their session at a designated start URL, then navigate from that start URL to any URL on a protected web site by clicking a link on another web page on that web site. Otherwise, requests to any URL that is not explicitly allowed are blocked.

denyURLAction Deny URL action types. (BLOCK | LOG | STATS | NONE)

denyURL A regular expression that designates a URL on the Deny URL list.

RefererHeaderCheck Enable validation of Referer headers. Referer validation ensures that a web form that a user sends to your web site originally came from your web site, not an outside attacker. Although this parameter is part of the Start URL check, referer validation protects against cross-site request forgery (CSRF) attacks, not Start URL attacks.

CSRFtagAction Cross-site request forgery tagging action types. (BLOCK | LEARN | LOG | STATS | NONE)

CSRFTag The web form originating URL.

CSRFFormActionURL The web form action URL.

crossSiteScriptingAction Cross-site scripting action types. (BLOCK | LEARN | LOG | STATS | NONE)

crossSiteScriptingTransformUnsafeHTML Enables transformation of unsafe HTML into safe HTML before forwarding a request to the web server.

crossSiteScriptingCheckCompleteURLs Tells the Application Firewall to check complete URLs rather than just the query portion of URLs for cross-site scripting violations.

crossSiteScripting The web form field name.

isRegex Is the web form field name a regular expression?

formActionURL The web form action URL.

exemptClosureURLsFromSecurityChecks Tells the Application Firewall to exempt closure URLs from security checks.

location Location of cross-site scripting exception - form field, header, cookie or URL.

valueType The web form value type.

valueExpression The web form value expression.

isValueRegex Is the web form field value a regular expression?

SQLInjectionAction SQL injection action types. (BLOCK | LEARN | LOG | STATS | NONE)

CMDInjectionAction CMD injection action types. (BLOCK | LOG | STATS | NONE)

SQLInjectionTransformSpecialChars Enables transformation of SQL special characters found in web forms into safe equivalents.

SQLInjectionOnlyCheckFieldsWithSQLChars Tells the Application Firewall to check form fields that contain SQL special characters only, rather than all form fields, for SQL injection violations.

SQLInjectionType Available SQL Injection types.

CMDInjectionType Available CMD Injection types.

SQLInjectionGrammar Check for SQL injection using SQL grammar

CMDInjectionGrammar Check for CMD injection using CMD grammar

SQLInjectionCheckSQLWildChars Check for form fields that contain SQL wild chars .

SQLInjection The web form field name.

isRegex Is the web form field name a regular expression?

formActionURL The web form action URL.

invalidPercentHandling Configure the method that the application firewall uses to handle percent-encoded names and values. Available settings function as follows:

- asp_mode - Microsoft ASP format.
- secure_mode - Secure format.

location Location of SQL injection exception - form field, header or cookie.

valueType The web form value type.

valueExpression The web form value expression.

isValueRegex Is the web form field value a regular expression?

RuleType Specifies rule type of binding

CMDInjection Name of the relaxed web form field/header/cookie

isRegex Is the relaxed web form field name/header/cookie a regular expression?

formActionURL The web form action URL.

location Location of command injection exception - form field, header or cookie.

valueType Type of the relaxed web form value

valueExpression The web form/header/cookie value expression.

isValueRegex Is the web form field/header/cookie value a regular expression?

fieldConsistencyAction Form Field Consistency action types. (BLOCK | LEARN | LOG | STATS | NONE)

fieldConsistency The web form field name.

isRegex Is the web form field name a regular expression?

formActionURL The web form action URL.

cookieConsistencyAction Cookie consistency action types. (BLOCK | LEARN | LOG | STATS | NONE)

cookieHijackingAction Cookie hijacking action types. (BLOCK | LOG | STATS | NONE)

cookieConsistency The name of the cookie to be checked.

isRegex Is the cookie name a regular expression?

cookieTransforms Perform the specified type of cookie transformation. Available settings function as follows:

- Encryption - Encrypt cookies.
- Proxying - Mask contents of server cookies by sending proxy cookie to users.
- Cookie flags - Flag cookies as HTTP only to prevent scripts on user's browser from accessing and possibly modifying them. CAUTION: Make sure that this parameter is set to ON if you are configuring any cookie transformations. If it is set to OFF, no cookie transformations are performed regardless of any other settings.

cookieEncryption Type of cookie encryption. Available settings function as follows:

- None - Do not encrypt cookies.
- Decrypt Only - Decrypt encrypted cookies, but do not encrypt cookies.
- Encrypt Session Only - Encrypt session cookies, but not permanent cookies.
- Encrypt All - Encrypt all cookies.

cookieProxying Proxies server cookies using the Application Firewall session

addCookieFlags Add the specified flags to cookies. Available settings function as follows:

- None - Do not add flags to cookies.
- HTTP Only - Add the HTTP Only flag to cookies, which prevents scripts from accessing cookies.
- Secure - Add Secure flag to cookies.
- All - Add both HTTPOnly and Secure flags to cookies.

bufferOverflowAction Buffer overflow action types. (BLOCK | LOG | STATS | NONE)

grpcAction gRPC validation

restAction REST validation

bufferOverflowMaxURLLength Maximum allowed length for URLs.

bufferOverflowMaxHeaderLength Maximum allowed length for HTTP headers.

bufferOverflowMaxCookieLength Maximum allowed length for cookies.

bufferOverflowMaxQueryLength Maximum allowed length for query string.

bufferOverflowMaxTotalHeaderLength Maximum allowed length for the total HTTP header length

fieldFormatAction Field format action types. (BLOCK | LEARN | LOG | STATS | NONE)

defaultFieldFormatType Name of the default field type, the field type that the Application Firewall will assign to a form field when no specific field type is assigned to that particular form field.

defaultFieldFormatMinLength Default field type minimum length setting.

defaultFieldFormatMaxLength Default field type maximum length setting.

fieldFormat Name of the form field to which a field format will be assigned.

isRegex Is the form field name a regular expression?

formActionURL Action URL of the form field to which a field format will be assigned.

fieldType The field type you are assigning to this form field.

fieldFormatMinLength The minimum allowed length for data in this form field.

fieldFormatMaxLength The maximum allowed length for data in this form field.

creditCardAction Credit Card action types. (BLOCK | LOG | STATS | NONE)

creditCard Credit card types. (AMEX | DINERSCLUB| DISCOVER | JBC | MASTERCARD | VISA)

creditCardMaxAllowed Maximum number of times a credit card number may be seen before action is taken.

creditCardXOut X-out credit card numbers.

doSecureCreditCardLogging Setting this option logs credit card numbers in the response when the match is found.

streaming Setting this option converts content-length form submission requests (requests with content-type "application/x-www-form-urlencoded" or "multipart/form-data") to chunked requests when atleast one of the following protections : Signatures, SQL injection protection, XSS protection, form field consistency protection, starturl closure, CSRF tagging, JSON SQL, JSON XSS, JSON DOS is enabled. Please make sure that the backend server accepts chunked requests before enabling this option. Citrix recommends enabling this option for large request sizes(>20MB).

trace Toggle the state of trace

safeObject Name of the Safe Object.

expression A regular expression that defines the Safe Object.

maxMatchLength Maximum match length for a Safe Object expression.

action Safe Object action types. (BLOCK | LOG | STATS | NONE)

requestContentType Default content-type for request messages.

responseContentType Default content-type for response messages.

XMLErrorObject URL for the xml error page

XMLErrorStatusCode Response status code associated with XML error page. Non-empty XML error object must be imported to the application firewall profile for the status code.

XMLErrorStatusMessage Response status message associated with XML error page

signatures Signatures for the profile

XMLFormatAction XML well-formed request action types. (BLOCK | LOG | STATS | NONE)

XMLDoSAction XML DOS action types. (BLOCK | LEARN | LOG | STATS | NONE)

XMLSQLInjectionAction XML SQL Injection action types. (BLOCK | LOG | STATS | NONE)

XMLSQLInjectionOnlyCheckFieldsWithSQLChars XML flag to check only fields with SQL characters.

XMLSQLInjectionType Available XML SQL Injection types.

XMLSQLInjectionCheckSQLWildChars XML flag to check for SQL wild chars.

XMLSQLInjectionParseComments Canonicalize SQL Comments in XML data.

XMLXSSAction XML cross-site scripting action types. (BLOCK | LOG | STATS | NONE)

XMLWSIAction XML WSI action types. (BLOCK | LEARN | LOG | STATS | NONE)

XMLAttachmentAction XML attachment action types. (BLOCK | LEARN | LOG | STATS | NONE)

XMLValidationAction XML message validation action types. (BLOCK | LOG | STATS | NONE)

XMLSOAPFaultAction XML SOAP fault filtering action types. (BLOCK | LOG | STATS | REMOVE | NONE)

XMLDoSURL XML DoS URL regular expression length.

XMLWSIURL XML WS-I URL regular expression length.

XMLValidationURL XML Validation URL regular expression.

XMLAttachmentURL XML attachment URL regular expression length.

XMLSQLInjection Exempt the specified URL from the XML SQL injection check. An XML SQL injection exemption (relaxation) consists of the following items:

- Name. Name to exempt, as a string or a PCRE-format regular expression.
- ISREGEX flag. REGEX if URL is a regular expression, NOTREGEX if URL is a fixed string.
- Location. ELEMENT if the injection is located in an XML element, ATTRIBUTE if located in an XML attribute.

isRegex Is the XML SQL Injection exempted field name a regular expression?

location Location of SQL injection exception - XML Element or Attribute.

XMLXSS Exempt the specified URL from the XML cross-site scripting (XSS) check. An XML cross-site scripting exemption (relaxation) consists of the following items:

- URL. URL to exempt, as a string or a PCRE-format regular expression.
- ISREGEX flag. REGEX if URL is a regular expression, NOTREGEX if URL is a fixed string.
- Location. ELEMENT if the attachment is located in an XML element, ATTRIBUTE if located in an XML attribute.

isRegex Is the XML XSS exempted field name a regular expression?

location Location of XSS injection exception - XML Element or Attribute.

XMLMaxElementDepthCheck State if XML Max element depth check is ON or OFF.

XMLMaxElementDepth Maximum nesting (depth) of XML elements. This check protects against documents that have excessive hierarchy depths.

XMLMaxElementNameLengthCheck State if XML Max element name length check is ON or OFF.

XMLMaxElementNameLength Specify the longest name of any element (including the expanded namespace) to protect against overflow attacks.

XMLMaxElementsCheck State if XML Max elements check is ON or OFF.

XMLMaxElements Specify the maximum number of XML elements allowed. Protects against overflow attacks.

XMLMaxElementChildrenCheck State if XML Max element children check is ON or OFF.

XMLMaxElementChildren Specify the maximum number of children allowed per XML element. Protects against overflow attacks.

XMLMaxNodesCheck State if XML Max nodes check is ON or OFF.

XMLMaxNodes Specify the maximum number of XML nodes. Protects against overflow attacks.

XMLMaxAttributesCheck State if XML Max attributes check is ON or OFF.

XMLMaxAttributes Specify maximum number of attributes per XML element. Protects against overflow attacks.

XMLMaxAttributeNameLengthCheck State if XML Max attribute name length check is ON or OFF.

XMLMaxAttributeNameLength Specify the longest name of any XML attribute. Protects against overflow attacks.

XMLMaxAttributeValueLengthCheck State if XML Max atribute value length is ON or OFF.

XMLMaxAttributeValueLength Specify the longest value of any XML attribute. Protects against overflow attacks.

XMLMaxCharDATALengthCheck State if XML Max CDATA length check is ON or OFF.

XMLMaxCharDATALength Specify the maximum size of CDATA. Protects against overflow attacks and large quantities of unparsed data within XML messages.

XMLMaxFileSizeCheck State if XML Max file size check is ON or OFF.

XMLMaxFileSize Specify the maximum size of XML messages. Protects against overflow attacks.

XMLMinFileSizeCheck State if XML Min file size check is ON or OFF.

XMLMinFileSize Enforces minimum message size.

XMLBlockPI State if XML Block PI is ON or OFF. Protects resources from denial of service attacks as SOAP messages cannot have processing instructions (PI) in messages.

XMLBlockDTD State if XML DTD is ON or OFF. Protects against recursive Document Type Declaration (DTD) entity expansion attacks. Also, SOAP messages cannot have DTDs in messages.

XMLBlockExternalEntities State if XML Block External Entities Check is ON or OFF. Protects against XML External Entity (XXE) attacks that force applications to parse untrusted external entities (sources) in XML documents.

XMLMaxEntityExpansionsCheck State if XML Max Entity Expansions Check is ON or OFF.

XMLMaxEntityExpansions Specify maximum allowed number of entity expansions. Protects aganist Entity Expansion Attack.

XMLMaxEntityExpansionDepthCheck State if XML Max Entity Expansions Depth Check is ON or OFF.

XMLMaxEntityExpansionDepth Specify maximum entity expansion depth. Protects aganist Entity Expansion Attack.

XMLMaxNamespacesCheck State if XML Max namespaces check is ON or OFF.

XMLMaxNamespaces Specify maximum number of active namespaces. Protects against overflow attacks.

XMLMaxNamespaceUriLengthCheck State if XML Max namespace URI length check is ON or OFF.

XMLMaxNamespaceUriLength Specify the longest URI of any XML namespace. Protects against overflow attacks.

XMLSOAPArrayCheck State if XML SOAP Array check is ON or OFF.

XMLMaxSOAPArraySize XML Max Total SOAP Array Size. Protects against SOAP Array Abuse attack.

XMLMaxSOAPArrayRank XML Max Individual SOAP Array Rank. This is the dimension of the SOAP array.

XMLWSIChecks Specify a comma separated list of relevant WS-I rule IDs. (R1140, R1141)

XMLRequestSchema XML Schema object for request validation .

XMLResponseSchema XML Schema object for response validation.

XMLWSDL WSDL object for soap request validation.

XMLAdditionalSOAPHeaders Allow addtional soap headers.

XMLEndPointCheck Modifies the behaviour of the Request URL validation w.r.t. the Service URL. If set to ABSOLUTE, the entire request URL is validated with the entire URL mentioned in Service of the associated WSDL. eg: Service URL: http://example.org/ExampleService, Request URL: http//example.com/ExampleService would FAIL the validation. If set to RELAIVE, only the non-hostname part of the request URL is validated against the non-hostname part of the Service URL. eg: Service URL: http://example.org/ExampleService, Request URL: http//example.com/ExampleService would PASS the validation.

XMLValidateSOAPEnvelope Validate SOAP Evelope only.

XMLValidateResponse Validate response message.

XMLMaxAttachmentSizeCheck State if XML Max attachment size Check is ON or OFF. Protects against XML requests with large attachment data.

XMLMaxAttachmentSize Specify maximum attachment size.

XMLAttachmentContentTypeCheck State if XML attachment content-type check is ON or OFF. Protects against XML requests with illegal attachments.

XMLAttachmentContentType Specify content-type regular expression.

builtin Indicates that a profile is a built-in entity.

builtin Indicates that a profile is a built-in entity.

feature The feature to be checked while applying this config

builtinType Type of built-in profiles

trustedLearningClients Specify trusted host/network IP

contentType A regular expression that designates a content-type on the content-types list.

excludeResContentType A regular expression that represents the content type of the response that are to be excluded from inspection.

CreditCardNumber The object expression that is to be excluded from safe commerce check

CreditCardNumberUrl The url for which the list of credit card numbers are needed to be bypassed from inspection

comment Comments associated with this profile.

percentDecodeRecursively Configure whether the application firewall should use percentage recursive decoding

multipleHeaderAction One or more multiple header actions. Available settings function as follows:

- Block - Block connections that have multiple headers.
- Log - Log connections that have multiple headers.
- KeepLast - Keep only last header when multiple headers are present.

Request headers inspected:

- Accept-Encoding
- Content-Encoding
- Content-Range
- Content-Type
- Host
- Range
- Referer

CLI users: To enable one or more actions, type "set appfw profile -multipleHeaderAction" followed by the actions to be enabled.

logExpression Name of LogExpression object.

expression LogExpression to log when violation happened on appfw profile

rfcprofile Object name of the rfc profile.

apispec Name of the API Specification.

protoFileObject Name of the imported proto file.

JSONErrorObject Name to the imported JSON Error Object to be set on application firewall profile.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my JSON error object" or 'my JSON error object'\).

JSONErrorStatusCode Response status code associated with JSON error page. Non-empty JSON error object must be imported to the application firewall profile for the status code.

JSONErrorStatusMessage Response status message associated with JSON error page

JSONDoSAction JSON DOS action types. (BLOCK | LOG | STATS | NONE)

JSONSQLInjectionAction JSON SQL Injection action types. (BLOCK | LOG | STATS | NONE)

JSONSQLInjectionType Available JSON SQL Injection types.

JSONSQLInjectionGrammar Check for SQL injection using SQL grammar in JSON

JSONCMDInjectionAction One or more JSON CMD Injection actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -JSONCMDInjectionAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -JSONCMDInjectionAction none".

JSONCMDInjectionType Available CMD injection types. -CMDSplChar : Checks for CMD Special Chars -CMDKeyword : Checks for CMD Keywords -CMDSplCharANDKeyword : Checks for both and blocks if both are found -CMDSplCharORKeyword : Checks for both and blocks if anyone is found, -None : Disables checking using both SQL Special Char and Keyword

JSONCMDInjectionGrammar Check for CMD injection using CMD grammar in JSON

JSONXSSAction JSON cross-site scripting action types. (BLOCK | LOG | STATS | NONE)

JSONSQLURL A regular expression that designates a URL on the Json SQL URL list for which SQL violations are relaxed. Enclose URLs in double quotes to ensure preservation of any embedded spaces or non-alphanumeric characters.

isRegex Is the key name a regular expression?

key An expression that designates a keyname on the JSON SQL URL for which SQL injection violations are relaxed.

valueType Type of the relaxed JSON SQL key value

valueExpression The JSON SQL key value expression.

isValueRegex Is the JSON SQL key value a regular expression?

JSONCMDURL A regular expression that designates a URL on the Json CMD URL list for which Command injection violations are relaxed. Enclose URLs in double quotes to ensure preservation of any embedded spaces or non-alphanumeric characters.

isRegex Is the key name a regular expression?

key An expression that designates a keyname on the JSON CMD URL for which Command injection violations are relaxed.

valueType Type of the relaxed JSON CMD key value

valueExpression The JSON CMD key value expression.

isValueRegex Is the JSON CMD key value a regular expression?

JSONXSSURL A regular expression that designates a URL on the Json XSS URL list for which XSS violations are relaxed. Enclose URLs in double quotes to ensure preservation of any embedded spaces or non-alphanumeric characters.

isRegex Is the key name a regular expression?

key An expression that designates a keyname on the JSON XSS URL for which XSS injection violations are relaxed.

valueType Type of the relaxed JSON XSS key value

valueExpression The JSON XSS key value expression.

isValueRegex Is the JSON XSS key value a regular expression?

JSONDoSURL The URL on which we need to enforce the specified JSON denial-of-service (JSONDoS) attack protections. An JSON DoS configuration consists of the following items:

- URL. PCRE-format regular expression for the URL.
- Maximum-document-length-check toggle. ON to enable this check, OFF to disable it.
- Maximum document length. Positive integer representing the maximum length of the JSON document.
- Maximum-container-depth-check toggle. ON to enable, OFF to disable.
- Maximum container depth. Positive integer representing the maximum container depth of the JSON document.
- Maximum-object-key-count-check toggle. ON to enable, OFF to disable.
- Maximum object key count. Positive integer representing the maximum allowed number of keys in any of the JSON object.
- Maximum-object-key-length-check toggle. ON to enable, OFF to disable.
- Maximum object key length. Positive integer representing the maximum allowed length of key in any of the JSON object.
- Maximum-array-value-count-check toggle. ON to enable, OFF to disable.
- Maximum array value count. Positive integer representing the maximum allowed number of values in any of the JSON array.
- Maximum-string-length-check toggle. ON to enable, OFF to disable.
- Maximum string length. Positive integer representing the maximum length of string in JSON.

JSONMaxDocumentLengthCheck State if JSON Max document length check is ON or OFF.

JSONMaxDocumentLength Maximum document length of JSON document, in bytes.

JSONMaxContainerDepthCheck State if JSON Max depth check is ON or OFF.

JSONMaxContainerDepth Maximum allowed nesting depth of JSON document. JSON allows one to nest the containers (object and array) in any order to any depth. This check protects against documents that have excessive depth of hierarchy.

JSONMaxObjectKeyCountCheck State if JSON Max object key count check is ON or OFF.

JSONMaxObjectKeyCount Maximum key count in the any of JSON object. This check protects against objects that have large number of keys.

JSONMaxObjectKeyLengthCheck State if JSON Max object key length check is ON or OFF.

JSONMaxObjectKeyLength Maximum key length in the any of JSON object. This check protects against objects that have large keys.

JSONMaxArrayLengthCheck State if JSON Max array value count check is ON or OFF.

JSONMaxArrayLength Maximum array length in the any of JSON object. This check protects against arrays having large lengths.

JSONMaxStringLengthCheck State if JSON Max string value count check is ON or OFF.

JSONMaxStringLength Maximum string length in the JSON. This check protects against strings that have large length.

fileUploadType FileUploadTypes to allow/deny.

formActionURL FileUploadTypes action URL.

isNameRegex Is field name a regular expression?

fileType FileUploadTypes file types.

fileUploadTypesAction One or more file upload types actions. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -fileUploadTypeAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -fileUploadTypeAction none".

verboseLogLevel Detailed Logging Verbose Log Level.

insertCookieSameSiteAttribute Configure whether application firewall should add samesite attribute for set-cookies

cookieSameSiteAttribute Cookie Samesite attribute added to support adding cookie SameSite attribute for all set-cookies including appfw session cookies. Default value will be "SameSite=Lax".

resourceId A "id" that identifies the rule.

SQLInjectionRuleType Specifies SQL Injection rule type: ALLOW/DENY. If ALLOW rule type is configured then allow list rules are used, if DENY rule type is configured then deny rules are used.

FakeAccountDetection Fake account detection flag : ON/OFF. If set to ON fake account detection in enabled on ADC, if set to OFF fake account detection is disabled.

fakeAccount Field name of the fake account rule.

isFieldNameRegex Is Fake Account Detection field name regex?

formURL The fake account detection URL.

formExpression A regular expression that defines the Fake Account.

tag A tag expression that defines the Fake Account.

GeoLocationLogging Enable Geo-Location Logging in CEF format logs for the profile.

CEFlogging Enable CEF format logs for the profile.

confidField Name of the form field to designate as confidential.

formURL URL of the web page that contains the web form.

isRegex Is Fake Account Detection field name regular expression?

blockKeywordAction Block Keyword action. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -blockKeywordAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -blockKeywordAction none".

blockKeyword Field name of the block keyword binding.

formURL The blockkeyword form action URL.

fieldName A block keyword field name

isNameRegex Is block keyword field name regular expression?

blockKeywordType block keyword type(literal|PCRE)

JSONBlockKeywordAction JSON Block Keyword action. Available settings function as follows:

- Block - Block connections that violate this security check.
- Log - Log violations of this security check.
- Stats - Generate statistics for this security check.
- None - Disable all actions for this security check.

CLI users: To enable one or more actions, type "set appfw profile -JSONBlockKeywordAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -JSONBlockKeywordAction none".

JSONBlockKeyword Field name of json block keyword binding

JSONBlockkeywordURL The json blockkeyword URL.

key JSON block keyword keyname

isRegex Is JSON blockkeyword key a regular expression?

JSONBlockKeywordType JSON block keyword type

bypasslist Enable bypass list for the profile.

bypasslist Bypass List Value

valueType Bypass List value type

ruleAction Bypass List Action

location Bypass List scan location

denylist Enable deny list for the profile.

denylist Deny List Value

valueType Deny List value type

ruleAction Deny List Action. Default value = REDIRECT

location Deny List scan location

sessionCookieName Name of the session cookie that the application firewall uses to track user sessions. Must begin with a letter or number, and can consist of from 1 to 31 letters, numbers, and the hyphen (-) and underscore (_) symbols.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cookie name" or 'my cookie name').

devno count

unbind appfw profile

Unbinds the specified exemption (relaxation) or rule from the specified application firewall profile. See the bind appfw profile command for a description of the parameters.

Synopsis

unbind appfw profile <name> (-startURL <expression> | -denyURL <expression> | (-fieldConsistency <string> <formActionURL>) | -cookieConsistency <string> | (-SQLInjection <string> <formActionURL> [-valueType <valueType>]) | (-CMDInjection <string> <formActionURL> [-valueType (Keyword | SpecialString)]) | (-CSRFTag <string> <CSRFFormActionURL>) | (-crossSiteScripting <string> <formActionURL> [-valueType <valueType>]) | (-fieldFormat <string> <formActionURL>) | -safeObject <string> | -trustedLearningClients <ip_addr|ipv6_addr> | (-JSONXSSURL <expression> [-key <expression>]) | (-JSONSQLURL <expression> [-key <expression>]) | (-JSONCMDURL <expression> [-key <expression>]) | -JSONDoSURL <expression> | -XMLDoSURL <expression> | -XMLWSIURL <expression> | -XMLValidationURL <expression> | -XMLAttachmentURL <expression> | (-XMLSQLInjection <string>) | (-XMLXSS <string>) | -contentType <expression> | -excludeResContentType <expression> | (-CreditCardNumber <expression> <CreditCardNumberUrl>) | -logExpression <string> | (-fileUploadType <expression> <formActionURL>) | (-fakeAccount <expression> -tag <expression>) | (-confidField <string> -formURL <expression>) | (-blockKeyword <expression> -fieldName <expression> -formURL <expression>) | (-JSONBlockKeyword <expression> -key <expression> -JSONBlockkeywordURL <expression>) | (-bypasslist <expression> -valueType <valueType>) | (-denylist <expression> -valueType <valueType>))

Arguments

name Name of the exemption (relaxation) or rule that you want to unbind.

startURL Start URL regular expression.

denyURL Deny URL regular expression.

fieldConsistency Form field name.

formActionURL Form action URL.

cookieConsistency Cookie name.

SQLInjection Form field, header or cookie name.

formActionURL Form action URL for exceptions in fields, or request URL for exceptions in headers and cookies.

location Location of SQL injection exception - form field, header or cookie.

Possible values: FORMFIELD, HEADER, COOKIE

valueType The web form value type.

Possible values: Keyword, SpecialString, Wildchar

valueExpression The web form value expression.

CMDInjection Form field, header or cookie name.

formActionURL Form action URL for exceptions in fields, or request URL for exceptions in headers and cookies.

location Location of command injection exception - form field, header or cookie.

Possible values: FORMFIELD, HEADER, COOKIE

valueType Type of the relaxed web form value

Possible values: Keyword, SpecialString

valueExpression The web form/header/cookie value expression.

CSRFTag CSRF Form origin URL. This binding is applicable to Profile Type: HTML.

CSRFFormActionURL CSRF form action URL.

crossSiteScripting Form field, header, cookie name or '.*' for url.

formActionURL Form action URL for exceptions in fields, or request URL for exceptions in headers, cookies and url.

location Location of cross-site scripting exception - form field, header, cookie or URL.

Possible values: FORMFIELD, HEADER, COOKIE, URL

valueType The web form value type.

Possible values: Tag, Attribute, Pattern

valueExpression The web form value expression.

fieldFormat Field format name.

formActionURL Form action URL.

safeObject Safe Object name.

trustedLearningClients Trusted learning Clients IP

JSONXSSURL A regular expression that designates a URL on the Json XSS URL list for which XSS violations are relaxed. Enclose URLs in double quotes to ensure preservation of any embedded spaces or non-alphanumeric characters.

key JSON XSS Key name

valueType JSON XSS value type. (Attribute | Pattern | Tag)

Possible values: Tag, Attribute, Pattern

valueExpression JSON XSS key value expressions consistituting expressions for attribute, pattern and tag

JSONSQLURL A regular expression that designates a URL on the Json SQL URL list for which SQL violations are relaxed. Enclose URLs in double quotes to ensure preservation of any embedded spaces or non-alphanumeric characters.

key JSON SQL Key name

valueType JSON SQL key value type. (Keyword | SpecialString)

Possible values: Keyword, SpecialString, Wildchar

valueExpression JSON SQL key value expressions consistituting expressions for Keyword and SpecialString

JSONCMDURL A regular expression that designates a URL on the Json CMD URL list for which Command injection violations are relaxed. Enclose URLs in double quotes to ensure preservation of any embedded spaces or non-alphanumeric characters.

key JSON CMD Key name

valueType JSON Command key value type. (Keyword | SpecialString)

Possible values: Keyword, SpecialString

valueExpression JSON_CMD key value expressions consistituting expressions for Keyword and SpecialString

JSONDoSURL The URL on which we need to enforce the specified JSON denial-of-service (JSONDoS) attack protections. An JSON DoS configuration consists of the following items:

- URL. PCRE-format regular expression for the URL.
- Maximum-document-length-check toggle. ON to enable this check, OFF to disable it.
- Maximum document length. Positive integer representing the maximum length of the JSON document.
- Maximum-container-depth-check toggle. ON to enable, OFF to disable.
- Maximum container depth. Positive integer representing the maximum container depth of the JSON document.
- Maximum-object-key-count-check toggle. ON to enable, OFF to disable.
- Maximum object key count. Positive integer representing the maximum allowed number of keys in any of the JSON object.
- Maximum-object-key-length-check toggle. ON to enable, OFF to disable.
- Maximum object key length. Positive integer representing the maximum allowed length of key in any of the JSON object.
- Maximum-array-value-count-check toggle. ON to enable, OFF to disable.
- Maximum array value count. Positive integer representing the maximum allowed number of values in any of the JSON array.
- Maximum-string-length-check toggle. ON to enable, OFF to disable.
- Maximum string length. Positive integer representing the maximum length of string in JSON.

XMLDoSURL XML DoS URL regular expression.

XMLWSIURL XML WS-I URL regular expression.

XMLValidationURL XML Message URL regular expression.

XMLAttachmentURL XML Attachment URL regular expression.

XMLSQLInjection Exempt the specified URL from the XML SQL injection check. An XML SQL injection exemption (relaxation) consists of the following items:

- Name. Name to exempt, as a string or a PCRE-format regular expression.
- ISREGEX flag. REGEX if URL is a regular expression, NOTREGEX if URL is a fixed string.
- Location. ELEMENT if the injection is located in an XML element, ATTRIBUTE if located in an XML attribute.

location Location of SQL injection exception - XML Element or Attribute. Default location is 'ELEMENT'

Possible values: ELEMENT, ATTRIBUTE Default value: AS_XMLLOCATION_ELEMENT

XMLXSS Exempt the specified URL from the XML cross-site scripting (XSS) check. An XML cross-site scripting exemption (relaxation) consists of the following items:

- URL. URL to exempt, as a string or a PCRE-format regular expression.
- ISREGEX flag. REGEX if URL is a regular expression, NOTREGEX if URL is a fixed string.
- Location. ELEMENT if the attachment is located in an XML element, ATTRIBUTE if located in an XML attribute.

location Location of XSS injection exception - XML Element or Attribute. Default location is 'ELEMENT'

Possible values: ELEMENT, ATTRIBUTE Default value: AS_XMLLOCATION_ELEMENT

contentType content-type regular expression.

excludeResContentType Response content type regular expression that are to be excluded from inspection.

CreditCardNumber The object expression that is to be excluded from safe commerce check.

CreditCardNumberUrl The url for which the list of credit card numbers are needed to be bypassed from inspection

logExpression Unbind specified logExpression to application firewall profile

fileUploadType Unbind the file upload types.

formActionURL Form action URL for making File Upload Type checks..

fileType FileUploadTypes file types.

fakeAccount Fake Account Detection rules.

tag A tag expression that defines the Fake Account.

formExpression A regular expression that defines the Fake Account.

formURL The fake account detection URL.

confidField Unbind confidential fields

formURL URL of the web page that contains the web form.

blockKeyword blockkeyword rules.

fieldName A block keyword field name

formURL The blockkeyword form action URL.

JSONBlockKeyword JSON blockkeyword rules.

key JSON block keyword keyname

JSONBlockkeywordURL The json blockkeyword URL.

bypasslist bypasslist rules

valueType Bypass List value type

Possible values: literal, PCRE, Expression Default value: literal Minimum value: 1

denylist denylist rules

valueType Deny List value type

Possible values: literal, PCRE, Expression Default value: literal Minimum value: 1

RuleType Specifies rule type of binding

Possible values: ALLOW, DENY

stat appfw profile

Displays statistics for the specified application firewall profile. If no profile is specified, displays abbreviated statistics for all profiles.

Synopsis

stat appfw profile

Arguments

name Name of the application firewall profile.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

requests (reqs) HTTP/HTTPS requests sent to your protected web servers via the Application Firewall.

Request Bytes (reqBytes) Number of bytes transfered for requests

responses (resps) HTTP/HTTPS responses sent by your protected web servers via the Application Firewall.

Response Bytes (resBytes) Number of bytes transfered for responses

aborts Incomplete HTTP/HTTPS requests aborted by the client before the Application Firewall could finish processing them.

redirects (redirect) HTTP/HTTPS requests redirected by the Application Firewall to a different Web page or web server. (HTTP 302)

Long Term Ave Response Time (ms) (longAvgRespTimePP) Average backend response time in milliseconds since reboot

Recent Ave Response Time (ms) (shortAvgRespTimePP) Average backend response time in milliseconds over the last 7 seconds

start URL (startURL) Number of Start URL security check violations seen by the Application Firewall.

deny URL (denyURL) Number of Deny URL security check violations seen by the Application Firewall.

referer header (refererHdr) Number of Referer Header security check violations seen by the Application Firewall.

buffer overflow (bufovfl) Number of Buffer Overflow security check violations seen by the Application Firewall.

Post Body Limit (postBodyLimit) Number of Post Body Limit security check violations seen by the Application Firewall.

cookie consistency (cookie) Number of Cookie Consistency security check violations seen by the Application Firewall.

cookie hijacking (cookiehijack) Number of Cookie Hijacking security violations seen by the Application Firewall.

CSRF form tag (csrf_tag) Number of Cross Site Request Forgery form tag security check violations seen by the Application Firewall.

HTML Cross-site scripting (xss) Number of HTML Cross-Site Scripting security check violations seen by the Application Firewall.

HTML SQL injection (sql) Number of HTML SQL Injection security check violations seen by the Application Firewall.

field format (fieldfmt) Number of Field Format security check violations seen by the Application Firewall.

field consistency (fieldcon) Number of Field Consistency security check violations seen by the Application Firewall.

credit card (ccard) Number of Credit Card security check violations seen by the Application Firewall.

safe object (safeobj) Number of Safe Object security check violations seen by the Application Firewall.

Signature Violations (sigs) Number of Signature violations seen by the Application Firewall.

content Type (contentType) Number of Content Type security check violations seen by the Application Firewall.

JSON Denial of Service (jsondosViolations) Number of JSON Denial-of-Service security check violations seen by the Application Firewall.

JSON SQL injection (jsonsqlViolations) Number of JSON SQL Injection security check violations seen by the Application Firewall.

JSON Cross-Site Scripting (jsonxssViolations) Number of JSON Cross-Site Scripting (XSS) security check violations seen by the Application Firewall.

JSON CMD injection (jsoncmdViolations) Number of JSON Command Injection security check violations seen by the Application Firewall.

File Upload Types (fileUploadTypes) Number of Field Upload Types security check violations seen by the Application Firewall.

Infer Content Type XML Payload (inferContentType) Number of Mismatched Content-Type in request with XML Payload security check violations seen by the Application Firewall.

HTML CMD Injection (cmd) Number of HTML Command Injection security check violations seen by the Application Firewall.

XML Format (wfcViolations) Number of XML Format security check violations seen by the Application Firewall.

XML Denial of Service (XDoS) (xdosViolations) Number of XML Denial-of-Service security check violations seen by the Application Firewall.

XML Message Validation (msgvalViolations) Number of XML Message Validation security check violations seen by the Application Firewall.

Web Services Interoperability (wsIViolations) Number of Web Services Interoperability (WS-I) security check violations seen by the Application Firewall.

XML SQL Injection (xmlSqlViolations) Number of XML SQL Injection security check violations seen by the Application Firewall.

XML Cross-Site Scripting (xmlXssViolations) Number of XML Cross-Site Scripting (XSS) security check violations seen by the Application Firewall.

XML Attachment (xmlAttachmentViolations) Number of XML Attachment security check violations seen by the Application Firewall.

SOAP Fault Violations (soapflt) Number of requests returning soap:fault from the backend server

XML Generic Violations (genflt) Number of requests returning XML generic violation from the backend server

HTML SQL injection (SQL grammar) (sqlgram) Number of HTML SQL Injection security check violations (reported by SQL grammar) seen by the Application Firewall.

JSON SQL injection (SQL grammar) (jsonsqlgramViolations) Number of JSON SQL Injection security check violations (reported by SQL grammar) seen by the Application Firewall.

Combined SQL injection (sqlcomb) Number of Combined SQL Injection security check violations seen by the Application Firewall.

Combined XXE (xxecomb) Number of combined XXE security check violations seen by the Application Firewall.

Combined Cross-site scripting (xsscomb) Number of combined Cross-Site Scripting security check violations seen by the Application Firewall.

Combined OWASP violations (owaspcomb) Number of combined OWASP security check violations seen by the Application Firewall.

HTML CMD injection (CMD grammar) (cmdgram) Number of HTML CMD Injection security check violations (reported by CMD grammar) seen by the Application Firewall.

JSON CMD injection (CMD grammar) (jsoncmdgramViolations) Number of JSON CMD Injection security check violations (reported by CMD grammar) seen by the Application Firewall.

HTML Block Keyword (blockkeyword) Number of HTML Block Keyword security check violations seen by the Application Firewall.

JSON Block Keyword (JSONblockkeyword) Number of JSON Block Keyword security check violations seen by the Application Firewall.

Total Violations (totperpr) Number of violations seen by the application firewall on per profile basis

start URL logs (startURLLog) Number of Start URL security check log messages generated by the Application Firewall.

deny URL logs (denyURLLog) Number of Deny URL security check log messages generated by the Application Firewall.

referer header logs (refererHdrLog) Number of Referer Header security check log messages generated by the Application Firewall.

buffer overflow logs (bufovflLog) Number of Buffer Overflow security check log messages generated by the Application Firewall.

gRPC Logs (gRPCLogs) Number of gRPC checks seen by the Application Firewall.

Post Body Limit Logs (postBodyLimitLogs) Number of Post Body Limit security check logs seen by the Application Firewall.

cookie consistency logs (cookieLog) Number of Cookie Consistency security check log messages generated by the Application Firewall.

cookie hijacking logs (cookiehijackLog) Number of Cookie Hijacking security violation log messages generated by the Application Firewall.

CSRF form tag logs (csrf_tagLog) Number of Cross Site Request Forgery form tag security check log messages generated by the Application Firewall.

HTML XSS logs (xssLog) Number of HTML Cross-Site Scripting security check log messages generated by the Application Firewall.

HTML XSS transform logs (xssXformLog) Number of HTML Cross-Site Scripting security check transform log messages generated by the Application Firewall.

HTML SQL Injection logs (sqlLog) Number of HTML SQL Injection security check log messages generated by the Application Firewall.

HTML SQL transform logs (sqlXformLog) Number of HTML SQL Injection security check transform log messages generated by the Application Firewall.

field format logs (fieldfmtLog) Number of Field Format security check log messages generated by the Application Firewall.

field consistency logs (fieldconLog) Number of Field Consistency security check log messages generated by the Application Firewall.

credit cards (ccardLog) Number of Credit Card security check log messages generated by the Application Firewall.

credit card transform logs (ccardXformLog) Number of Credit Card security check transform log messages generated by the Application Firewall.

safe object logs (safeobjLog) Number of Safe Object security check log messages generated by the Application Firewall.

Signature logs (sigs) Number of Signature log messages generated by the Application Firewall.

content Type logs (contenttypeLog) Number of Content type security check log messages generated by the Application Firewall.

JSON Denial of Service logs (jsondosLogs) Number of JSON Denial-of-Service security check log messages generated by the Application Firewall.

JSON SQL injection logs (jsonsqlLogs) Number of JSON SQL Injection security check log messages generated by the Application Firewall.

JSON Cross-Site Scripting logs (jsonxssLogs) Number of JSON Cross-Site Scripting (XSS) security check log messages generated by the Application Firewall.

JSON CMD injection logs (jsoncmdLogs) Number of JSON Command Injection security check log messages generated by the Application Firewall.

file upload types logs (fileUploadTypesLog) Number of File Upload Types security check log messages generated by the Application Firewall.

Infer Content Type XML Payload Logs (inferContentTypeXMLPayloadLog) Number of Mismatched Content-Type in request with XML Payload security check logs seen by the Application Firewall.

HTML Command Injection logs (cmdLog) Number of HTML Command Injection security check log messages generated by the Application Firewall.

XML Format logs (wfcLogs) Number of XML Format security check log messages generated by the Application Firewall.

XML Denial of Service(XDoS) logs (xdosLogs) Number of XML Denial-of-Service security check log messages generated by the Application Firewall.

XML Message Validation logs (msgvalLogs) Number of XML Message Validation security check log messages generated by the Application Firewall.

WSI logs (wsiLogs) Number of Web Services Interoperability (WS-I) security check log messages generated by the Application Firewall.

XML SQL Injection logs (xmlSqlLogs) Number of XML SQL Injection security check log messages generated by the Application Firewall.

XML XSS logs (xmlXssLogs) Number of XML Cross-Site Scripting (XSS) security check log messages generated by the Application Firewall.

XML Attachment logs (xmlAttachmentLogs) Number of XML Attachment security check log messages generated by the Application Firewall.

SOAP Fault logs (soapfltLogs) Number of requests generating soap:fault log messages

XML Generic logs (genfltLog) Number of requests generating XML Generic log messages

HTML SQL Injection logs (SQL grammar) (sqlGramLog) Number of HTML SQL Injection security check log messages (reported by SQL grammar) generated by the Application Firewall.

JSON SQL injection logs (SQL grammar) (jsonsqlGramLogs) Number of JSON SQL Injection security check log messages (reported by SQL grammar) generated by the Application Firewall.

HTML CMD Injection logs (CMD grammar) (cmdGramLog) Number of HTML CMD Injection security check log messages (reported by CMD grammar) generated by the Application Firewall.

JSON CMD injection logs (CMD grammar) (jsoncmdGramLogs) Number of JSON CMD Injection security check log messages (reported by CMD grammar) generated by the Application Firewall.

HTML Block Keyword logs (blockKeywordLog) Number of HTML Block Keyword security check log messages generated by the Application Firewall.

JSON Block Keyword logs (JSONblockKeywordLog) Number of JSON Block Keyword security check log messages generated by the Application Firewall.

Total log messages (totlogperpr) Number of log messages generated by the application firewall on per profile basis

HTTP Client Errors (4xx Resp) (4xxResps) Number of requests returning HTTP 4xx from the backend server

HTTP Server Errors (5xx Resp) (5xxResps) Number of requests returning HTTP 5xx from the backend server

Config Start URL Closure (cfgstarturlclosure) Number of profiles with Start URL Closure enabled in the Application Firewall.

Config Cookie Transforms (cfgcookietransforms) Number of profiles with Config Cookie Transforms enabled in the Application Firewall.

Config CrossSite Scripting Transform Unsafe HTML (cfgcrosssitescriptingtransformunsafehtml) Number of profiles with CrossSite Scripting Transform Unsafe HTML enabled in the Application Firewall.

Config CrossSite Scripting Check Complete URLs (cfgcrosssitescriptingcheckcompleteurls) Number of profiles with CrossSite Scripting Check Complete URLs enabled in the Application Firewall.

Config SQL Injection Grammar (cfgsqlinjectiongrammar) Number of profiles with SQL Injection Grammar enabled in the Application Firewall.

Config SQL Injection Transform Special Chars (cfgsqlinjectiontransformspecialchars) Number of profiles with SQL Injection Transform Special Chars enabled in the Application Firewall.

Config SQL Injection Check SQL Wild Chars (cfgsqlinjectionchecksqlwildchars) Number of profiles with SQL Injection Check SQL Wild Chars enabled in the Application Firewall.

Config Credit Card XOut (cfgcreditcardxout) Number of profiles with Credit Card XOut enabled in the Application Firewall.

Config Do Secure Credit Card Logging (cfgdosecurecreditcardlogging) Number of profiles with Do Secure Credit Card Logging enabled in the Application Firewall.

Config Streaming (cfgstreaming) Number of profiles with Streaming enabled in the Application Firewall.

Config Trace (cfgtrace) Number of profiles with Trace enabled in the Application Firewall.

Config JSON SQL Injection Grammar (cfgjsonsqlinjectiongrammar) Number of profiles with JSON SQL Injection Grammar enabled in the Application Firewall.

Config XML SQL Injection Check SQL Wild Chars (cfgxmlsqlinjectionchecksqlwildchars) Number of profiles with XML SQL Injection Check SQL Wild Chars enabled in the Application Firewall.

Config Use HTML Error Object (cfgusehtmlerrorobject) Number of profiles with Use HTML Error Object enabled in the Application Firewall.

Config Log Every Policy Hit (cfglogeverypolicyhit) Number of profiles with Log Every Policy Hit enabled in the Application Firewall.

Config Exempt Closure URLs From Security Checks (cfgexemptclosureurlsfromsecuritychecks) Number of profiles with Exempt Closure URLs From Security Checks enabled in the Application Firewall.

Config Canonicalize HTML Response (cfgcanonicalizehtmlresponse) Number of profiles with Canonicalize HTML Response enabled in the Application Firewall.

Config Enable Form Tagging (cfgenableformtagging) Number of profiles with Enable Form Tagging enabled in the Application Firewall.

Config Sessionless URL Closure (cfgsessionless_url_closure) Number of profiles with Sessionless URL Closure enabled in the Application Firewall.

Config Semicolon Field Separator (cfgsemicolonfieldseparator) Number of profiles with Semicolon Field Separator enabled in the Application Firewall.

Config Exclude File Upload From Checks (cfgexcludefileuploadfromchecks) Number of profiles with Exclude File Upload From Checks enabled in the Application Firewall.

Config Check Request Headers (cfgcheckrequestheaders) Number of profiles with Check Request Headers enabled in the Application Firewall.

Config Optimize Partial Reqs (cfgoptimizepartialreqs) Number of profiles with Optimize Partial Reqs enabled in the Application Firewall.

Config URL Decode Request Cookies (cfgurldecoderequestcookies) Number of profiles with URL Decode Request Cookies enabled in the Application Firewall.

Config Percent Decode Recursively (cfgpercentdecoderecursively) Number of profiles with Percent Decode Recursively enabled in the Application Firewall.

Config Insert Cookie SameSite Attribute (cfginsertcookiesamesiteattribute) Number of profiles with Insert Cookie SameSite Attribute enabled in the Application Firewall.

Config Fake Account Detection (cfgfakeaccountdetection) Number of profiles with Fake Account Detection enabled in the Application Firewall.

Example

stat appfw profile

Related Commands

- stat appfw policylabel

appfw-protofile

The following operations can be performed on "appfw-protofile":

import| update| show| rm|

import appfw protofile

Imports a gRPC schema file from specified location.

Synopsis

import appfw protofile <src> <name>

Arguments

src Indicates source path of the gRPC schema file.

name Source path of the gRPC schema file.

overwrite Overwrite any existing gRPC schema object of the same name.

comment Comments associated with this gRPC schema file.

update appfw protofile

Updates the specified gRPC schema file object.

Synopsis

update appfw protofile <name>

Arguments

name Name of the gRPC schema object.

Example

update appfw protofile grpc-schema

show appfw protofile

Displays the specified gRPC schema object.

Synopsis

show appfw protofile

Arguments

name Name of the gRPC schema object.

Output

response gRPC import object response contents.

src Indicates the source of the gRPC schema file as a URL of the form:

```
&lt;protocol&gt;://&lt;host&gt;[:&lt;port&gt;][/&lt;path&gt;]
```

Where: <protocol> is http or https. <host> is the DNS name or IP address of the http or https server. <port> is the port number of the server. If omitted, the default port for http or https will be used. <path> is the path of the file on the server.

Example

show appfw protofile <name>

rm appfw protofile

Removes the named gRPC schema object.

Synopsis

rm appfw protofile <name>

Arguments

name Indicates name of the gRPC schema object to be removed.

Example

rm appfw protofile <name>

appfw-settings

The following operations can be performed on "appfw-settings":

unset| set| show|

unset appfw settings

Use this command to remove appfw settings settings.Refer to the set appfw settings command for meanings of the arguments.

Synopsis

unset appfw settings

set appfw settings

Modifies the global application firewall settings. The global settings apply to all application firewall profiles.

Synopsis

set appfw settings [-proxyUsername <string>]

Arguments

defaultProfile Profile to use when a connection does not match any policy. Default setting is APPFW_BYPASS, which sends unmatched connections back to the Citrix ADC without attempting to filter them further. Default value: APPFW_BYPASS

undefAction Profile to use when an application firewall policy evaluates to undefined (UNDEF). An UNDEF event indicates an internal error condition. The APPFW_BLOCK built-in profile is the default setting. You can specify a different built-in or user-created profile as the UNDEF profile. Default value: APPFW_BLOCK

sessionTimeout Timeout, in seconds, after which a user session is terminated. Before continuing to use the protected web site, the user must establish a new session by opening a designated start URL. Default value: 900 Minimum value: 1 Maximum value: 65535

learnRateLimit Maximum number of connections per second that the application firewall learning engine examines to generate new relaxations for learning-enabled security checks. The application firewall drops any connections above this limit from the list of connections used by the learning engine. Default value: 400 Minimum value: 1 Maximum value: 1000

sessionLifetime Maximum amount of time (in seconds) that the application firewall allows a user session to remain active, regardless of user activity. After this time, the user session is terminated. Before continuing to use the protected web site, the user must establish a new session by opening a designated start URL. Default value: 0 Minimum value: 0 Maximum value: 2147483647

sessionCookieName Name of the session cookie that the application firewall uses to track user sessions. Must begin with a letter or number, and can consist of from 1 to 31 letters, numbers, and the hyphen (-) and underscore (_) symbols.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cookie name" or 'my cookie name'). Default value: NS_S_AS_DEFAULT_COOKIE_NAME

clientIPLoggingHeader Name of an HTTP header that contains the IP address that the client used to connect to the protected web site or service.

importSizeLimit Cumulative total maximum number of bytes in web forms imported to a protected web site. If a user attempts to upload files with a total byte count higher than the specified limit, the application firewall blocks the request. Default value: 134217728 Minimum value: 1 Maximum value: 268435456

signatureAutoUpdate Flag used to enable/disable auto update signatures

Possible values: ON, OFF Default value: OFF

signatureUrl URL to download the mapping file from server Default value: https://s3.amazonaws.com/NSAppFwSignatures/SignaturesMapping.xml

cookiePostEncryptPrefix String that is prepended to all encrypted cookie values. Default value: NS_S_AS_DEFAULT_CKI_POST_ENCRYPT_PREFIX

GeoLocationLogging Enable Geo-Location Logging in CEF format logs.

Possible values: ON, OFF Default value: OFF

CEFLogging Enable CEF format logs.

Possible values: ON, OFF Default value: OFF

entityDecoding Transform multibyte (double- or half-width) characters to single width characters.

Possible values: ON, OFF Default value: OFF

useConfigurableSecretKey Use configurable secret key in AppFw operations

Possible values: ON, OFF Default value: OFF

sessionLimit Maximum number of sessions that the application firewall allows to be active, regardless of user activity. After the max_limit reaches, No more user session will be created . Default value: 100000 Minimum value: 0 Maximum value: 500000

malformedReqAction flag to define action on malformed requests that application firewall cannot parse Default value: AS_DEFAULT_DISPOSITION

CentralizedLearning Flag used to enable/disable ADM centralized learning

Possible values: ON, OFF Default value: OFF

proxyServer Proxy Server IP to get updated signatures from AWS.

proxyPort Proxy Server Port to get updated signatures from AWS. Default value: 8080

proxyUsername Proxy Username

proxyPassword Password with which proxy user logs on.

show appfw settings

Displays the current application firewall global settings.

Synopsis

show appfw settings

Arguments

Output

defaultProfile Profile to use when a connection does not match any policy. Default setting is APPFW_BYPASS, which sends unmatched connections back to the Citrix ADC without attempting to filter them further.

undefAction Profile to use when an application firewall policy evaluates to undefined (UNDEF). An UNDEF event indicates an internal error condition. The APPFW_BLOCK built-in profile is the default setting. You can specify a different built-in or user-created profile as the UNDEF profile.

sessionTimeout Session timeout (in seconds).

learnRateLimit Learn messages rate limit value (in messages per second).

sessionLifetime Session lifetime (in seconds). Zero means no limit.

sessionCookieName Name of the session cookie that the application firewall uses to track user sessions. Must begin with a letter or number, and can consist of from 1 to 31 letters, numbers, and the hyphen (-) and underscore (_) symbols.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cookie name" or 'my cookie name').

clientIPLoggingHeader Name of header that holds downstream IP address for logging purposes.

importSizeLimit Cumulative total maximum number of bytes in web forms imported to a protected web site. If a user attempts to upload files with a total byte count higher than the specified limit, the application firewall blocks the request.

signatureAutoUpdate Flag used to enable/disable auto update signatures

signatureUrl URL to download the mapping file from server

cookiePostEncryptPrefix String that is prepended to all encrypted cookie values.

logMalformedReq Log requests that are so malformed that application firewall parsing doesn't occur.

GeoLocationLogging Enable Geo-Location Logging in CEF format logs.

CEFLogging Enable CEF format logs.

entityDecoding Transform multibyte (double- or half-width) characters to single width characters.

useConfigurableSecretKey Use configurable secret key in AppFw operations

sessionLimit Maximum number of sessions that the application firewall allows to be active, regardless of user activity. After the max_limit reaches, No more user session will be created .

appEnforceSessionLimit Let application firewall enforce session limits. Available settings are as follows:

- ON - Application firewall enforces session limits.
- OFF - DHT framework enforces session limits

malformedReqAction flag to define action on malformed requests that application firewall cannot parse

learning Global learning option that overrides the profile level learning. Available settings are as follows:

- ON - Honor all profile level learn settings.
- OFF - Avoids learning for all profiles ignoring profile level learn setting.

CentralizedLearning Flag used to enable/disable ADM centralized learning

proxyServer Proxy Server IP to get updated signatures from AWS.

proxyPort Proxy Server Port to get updated signatures from AWS.

proxyUsername Proxy Username

proxyPassword Password with which proxy user logs on.

builtin Flag to determine if application firewall settings is built-in or not

feature The feature to be checked while applying this config

appfw-signatures

The following operations can be performed on "appfw-signatures":

show| update| rm| import|

show appfw signatures

Displays the specified signatures object. If no signatures object is specified, displays all signatures objects defined on the Citrix ADC.

Synopsis

show appfw signatures

Arguments

name Name of the signature object.

Output

response src URL (protocol, host, path, and file name) for the location at which to store the imported signatures object. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

Example

show appfw signatures

update appfw signatures

Updates the specified signatures object from the source.

Synopsis

update appfw signatures <name>

Arguments

name Name of the signatures object to update.

Example

update signatures my-signatures

rm appfw signatures

Removes the specified signature object from the application firewall.

Synopsis

rm appfw signatures <name>

Arguments

name Name of the signature object.

Example

rm signatures <name>

import appfw signatures

Imports the specified signatures object to the Citrix ADC and assigns it the specified name.

Synopsis

import appfw signatures <src> <name> [-merge]

Arguments

src URL (protocol, host, path, and file name) for the location at which to store the imported signatures object. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

name Name to assign to the signatures object on the Citrix ADC.

xslt XSLT file source.

comment Any comments to preserve information about the signatures object.

overwrite Overwrite any existing signatures object of the same name.

merge Merges the existing Signature with new signature rules

preservedefactions preserves def actions of signature rules

sha1 File path for sha1 file to validate signature file

VendorType Third party vendor type for which WAF signatures has to be generated.

Possible values: Snort

autoEnableNewSignatures Flag used to enable/disable auto enable new signatures

Possible values: ON, OFF Default value: OFF

ruleID Signature rule IDs to be Enabled/Disabled Minimum value: 1 Maximum value: 2000000

category Signature category to be Enabled/Disabled

Enabled Flag used to enable/disable enable signature rule IDs/Signature Category

Possible values: ON, OFF Default value: ON

Action Signature action Default value: AS_SIGNATURE_DISPOSITION

Example

import signatures http://www.example.com/ns/signatures.xml my-signature

appfw-stats

The following operations can be performed on "appfw-stats":

show appfw stats

show appfw stats is an alias for stat appfw

Synopsis

show appfw stats - alias for 'stat appfw'

appfw-transactionRecords

The following operations can be performed on "appfw-transactionRecords":

show appfw transactionRecords

Display an application firewall transaction record.

Synopsis

show appfw transactionRecords

Arguments

Output

httpTransactionId The http transaction identifier.

packetEngineId The packet engine identifier.

AppFwSessionId The session identifier set by the Application Firewall to track the user session.

profileName Application Firewall profile name.

url Request URL

clientip The IP address of client.

destIP The IP address of destination.

startTime Conveys time at which request processing started.

endTime Conveys time at which request processing end.

requestContentLength The content length of request.

requestYields The number of times yielded during request processing to send heart beat packets.

requestMaxProcessingTime The maximum processing time across yields during request processing.

responseContentLength The content length of response.

responseYields The number of times yielded during response processing to send heart beat packets.

responseMaxProcessingTime The maximum processing time across yields during response processing.

flag Record flags.

devno count stateflag

appfw-urlEncodedFormContentType

The following operations can be performed on "appfw-urlEncodedFormContentType":

rm| show| add|

rm appfw urlEncodedFormContentType

Remove urlencoded form content type.

Synopsis

rm appfw urlEncodedFormContentType <UrlencodedFormContenttypevalue>

Arguments

UrlencodedFormContenttypevalue Content type to be classified as urlencoded form

show appfw urlEncodedFormContentType

Display all URLENCODED_FORM content types.

Synopsis

show appfw urlEncodedFormContentType

Arguments

UrlencodedFormContenttypevalue Content type to be classified as urlencoded form

Output

isRegex Is urlencoded form content type a regular expression?

builtin Flag to determine if urlencoded form contenttype is built-in or not

feature The feature to be checked while applying this config

devno count stateflag

add appfw urlEncodedFormContentType

Add urlencoded form content type. This will classify a request/response with the specified content type as urlencoded form

Synopsis

add appfw urlEncodedFormContentType <UrlencodedFormContenttypevalue>

Arguments

UrlencodedFormContenttypevalue Content type to be classified as urlencoded form

isRegex Is urlencoded form content type a regular expression?

Possible values: REGEX, NOTREGEX Default value: NOTREGEX

appfw-wsdl

The following operations can be performed on "appfw-wsdl":

import| rm| show|

import appfw wsdl

Imports the specified WSDL file to the application firewall.

Synopsis

import appfw wsdl <src> <name>

Arguments

src URL (protocol, host, path, and name) of the WSDL file to be imported is stored. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

name Name to assign to the WSDL on the Citrix ADC.

comment Any comments to preserve information about the WSDL.

overwrite Overwrite any existing WSDL of the same name.

Example

import appfw wsdl http://www.webservicex.net/stockquote.asmx?wsdl stockquote

rm appfw wsdl

Removes the specified imported WSDL file from the application firewall.

Synopsis

rm appfw wsdl <name>

Arguments

name Name of the WSDL file to remove.

Example

rm wsdl <name>

show appfw wsdl

Removes the specified imported WSDL file.

Synopsis

show appfw wsdl

Arguments

name Name of the WSDL file to display.

Output

response

Example

show appfw wsdl

appfw-xmlerrorpage

The following operations can be performed on "appfw-xmlerrorpage":

import| show| update| rm|

import appfw xmlerrorpage

Imports the specified XML error page to the Citrix ADC and assigns it the specified name.

Synopsis

import appfw xmlerrorpage <src> <name>

Arguments

src URL (protocol, host, path, and name) for the location at which to store the imported XML error object. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

name Name to assign to the XML error object on the Citrix ADC.

comment Any comments to preserve information about the XML error object.

overwrite Overwrite any existing XML error object of the same name.

Example

import xmlerrorpage http://www.example.com/errorpage.xml my-xml-error-page

show appfw xmlerrorpage

Displays the specified XML error object. If no XML error page object is specified, displays a list of all XML error objects on the Citrix ADC.

Synopsis

show appfw xmlerrorpage

Arguments

name Name of the XML error object.

Output

response src URL (protocol, host, path, and name) for the location at which to store the imported XML error object. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

Example

show appfw xmlerrorpage

update appfw xmlerrorpage

Updates the specified XML error object from the source.

Synopsis

update appfw xmlerrorpage <name>

Arguments

name Name of the XML error object.

Example

update xmlerrorpage my-xml-error-page

rm appfw xmlerrorpage

Removes the object imported by import xmlerrorpage.

Synopsis

rm appfw xmlerrorpage <name>

Arguments

name Indicates name of the imported xml error page to be removed.

Example

rm xmlerrorpage <name>

appfw-xmlschema

The following operations can be performed on "appfw-xmlschema":

show| rm| import|

show appfw xmlschema

Displays the specified XML Schema object. If no object is specified, displays all XML Schema objects on the Citrix ADC.

Synopsis

show appfw xmlschema

Arguments

name Name of the XML Schema object to display.

Output

response

Example

show appfw xmlschema

rm appfw xmlschema

Removes the specified XML Schema object from the application firewall.

Synopsis

rm appfw xmlschema <name>

Arguments

name Name of the XML Schema object to remove.

Example

rm xmlschema <name>

import appfw xmlschema

Imports the specified XML Schema to the Citrix ADC and assigns it the specified name.

Synopsis

import appfw xmlschema <src> <name>

Arguments

src URL (protocol, host, path, and file name) for the location at which to store the imported XML Schema. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

name Name to assign to the XML Schema object on the Citrix ADC.

comment Any comments to preserve information about the XML Schema object.

overwrite Overwrite any existing XML Schema object of the same name.

Example

import xmlschema http://schemas.xmlsoap.org/soap/envelope/ soap

appfw

The following operations can be performed on "appfw":

stat appfw

Displays application firewall statistics.

Synopsis

stat appfw

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

total log messages (totlogs) Total number of security check log messages generated by the Application Firewall.

total violations (totviols) Total number of security check violations seen by the Application Firewall.

Recent Ave Response Time (ms) (shortAvgRespTime) Average backend response time in milliseconds over the last 7 seconds

Long Term Ave Response Time (ms) (longAvgRespTime) Average backend response time in milliseconds since reboot

requests (reqs) HTTP/HTTPS requests sent to your protected web servers via the Application Firewall.

Request Bytes (reqBytes) Number of bytes transfered for requests

responses (resps) HTTP/HTTPS responses sent by your protected web servers via the Application Firewall.

Response Bytes (resBytes) Number of bytes transfered for responses

aborts Incomplete HTTP/HTTPS requests aborted by the client before the Application Firewall could finish processing them.

redirects (redirect) HTTP/HTTPS requests redirected by the Application Firewall to a different Web page or web server. (HTTP 302)

Traps Dropped (trapsDr) AppFirewall SNMP traps dropped due to time limit.

start URL (startURL) Number of Start URL security check violations seen by the Application Firewall.

deny URL (denyURL) Number of Deny URL security check violations seen by the Application Firewall.

referer header (refererHdr) Number of Referer Header security check violations seen by the Application Firewall.

buffer overflow (bufovfl) Number of Buffer Overflow security check violations seen by the Application Firewall.

gRPC Violation (gRPCViolation) Number of gRPC security check violations seen by the Application Firewall.

Post Body Limit (postBodyLimit) Number of Post Body Limit security check violations seen by the Application Firewall.

cookie consistency (cookie) Number of Cookie Consistency security check violations seen by the Application Firewall.

cookie hijacking (cookie_hijack) Number of Cookie Hijacking security violations seen by the Application Firewall.

CSRF form tag (csrf_tag) Number of Cross Site Request Forgery form tag security check violations seen by the Application Firewall.

HTML Cross-site scripting (xss) Number of HTML Cross-Site Scripting security check violations seen by the Application Firewall.

HTML SQL injection (sql) Number of HTML SQL Injection security check violations seen by the Application Firewall.

field format (fieldfmt) Number of Field Format security check violations seen by the Application Firewall.

field consistency (fieldcon) Number of Field Consistency security check violations seen by the Application Firewall.

File Upload Types (fileUploadTypes) Number of Field Upload Types security check violations seen by the Application Firewall.

Infer Content Type XML Payload (inferContentType) Number of Mismatched Content-Type in request with XML Payload security check violations seen by the Application Firewall.

credit card (ccard) Number of Credit Card security check violations seen by the Application Firewall.

safe object (safeobj) Number of Safe Object security check violations seen by the Application Firewall.

Signature Violations (sigs) Number of Signature violations seen by the Application Firewall.

content Type (contentType) Number of Content type security check violations seen by the Application Firewall.

HTML CMD injection (cmd) Number of HTML CMD Injection security check violations seen by the Application Firewall.

JSON Denial of Service (jsondosViolations) Number of JSON Denial-of-Service security check violations seen by the Application Firewall.

JSON SQL injection (jsonsqlViolations) Number of JSON SQL Injection security check violations seen by the Application Firewall.

JSON Cross-Site Scripting (jsonxssViolations) Number of JSON Cross-Site Scripting (XSS) security check violations seen by the Application Firewall.

JSON CMD injection (jsoncmdViolations) Number of JSON Command Injection security check violations seen by the Application Firewall.

XML Format (wfcViolations) Number of XML Format security check violations seen by the Application Firewall.

XML Denial of Service (XDoS) (xdosViolations) Number of XML Denial-of-Service security check violations seen by the Application Firewall.

XML Message Validation (msgvalViolations) Number of XML Message Validation security check violations seen by the Application Firewall.

Web Services Interoperability (wsIViolations) Number of Web Services Interoperability (WS-I) security check violations seen by the Application Firewall.

XML SQL Injection (xmlSqlViolations) Number of XML SQL Injection security check violations seen by the Application Firewall.

XML Cross-Site Scripting (xmlXssViolations) Number of XML Cross-Site Scripting (XSS) security check violations seen by the Application Firewall.

XML Attachment (xmlAttachmentViolations) Number of XML Attachment security check violations seen by the Application Firewall.

SOAP Fault Violations (soapflt) Number of requests returning soap:fault from the backend server

XML Generic Violations (genflt) Number of requests returning XML generic error from the backend server

HTML SQL injection (SQL grammar) (sqlgram) Number of HTML SQL Injection security check violations (using SQL grammar) seen by the Application Firewall.

JSON SQL injection (SQL grammar) (jsonsqlViolations) Number of JSON SQL Injection security check violations (reported using SQL grammar) seen by the Application Firewall.

Combined SQL injection (sqlcomb) Number of combined SQL Injection security check violations seen by the Application Firewall.

Combined XXE (xxecomb) Number of combined XXE security check violations seen by the Application Firewall.

Commbined Cross-Site Scripting (xsscomb) Number of combined Cross-Site Scripting security check violations seen by the Application Firewall.

Commbined OWASP violations (owaspcomb) Number of combined OWASP security check violations seen by the Application Firewall.

HTML CMD injection (CMD grammar) (cmdgram) Number of HTML CMD Injection security check violations (using SQL grammar) seen by the Application Firewall.

JSON CMD injection (CMD grammar) (jsoncmdViolations) Number of JSON CMD Injection security check violations (reported using CMD grammar) seen by the Application Firewall.

block keyword (blockKeyword) Number of Block Keyword security check violations seen by the Application Firewall.

JSON block keyword (JSONblockKeyword) Number of JSON Block Keyword security check violations seen by the Application Firewall.

start URL logs (startURLLog) Number of Start URL security check log messages generated by the Application Firewall.

deny URL logs (denyURLLog) Number of Deny URL security check log messages generated by the Application Firewall.

referer header logs (refererHdrLog) Number of Referer Header security check log messages generated by the Application Firewall.

buffer overflow logs (bufovflLog) Number of Buffer Overflow security check log messages generated by the Application Firewall.

gRPC Logs (gRPCLog) Number of gRPC security check logs seen by the Application Firewall.

Post Body Limit Logs (postBodyLimitLogs) Number of Post Body Limit security check logs seen by the Application Firewall.

cookie consistency logs (cookieLog) Number of Cookie Consistency security check log messages generated by the Application Firewall.

cookie hijacking logs (cookiehijackLog) Number of Cookie Hijacking security violation log messages generated by the Application Firewall.

CSRF form tag logs (csrf_tagLog) Number of Cross Site Request Forgery form tag security check log messages generated by the Application Firewall.

HTML XSS logs (xssLog) Number of HTML Cross-Site Scripting security check log messages generated by the Application Firewall.

HTML XSS transform logs (xssXformLog) Number of HTML Cross-Site Scripting security check transform log messages generated by the Application Firewall.

HTML SQL logs (sqlLog) Number of HTML SQL Injection security check log messages generated by the Application Firewall.

HTML SQL transform logs (sqlXformLog) Number of HTML SQL Injection security check transform log messages generated by the Application Firewall.

field format logs (fieldfmtLog) Number of Field Format security check log messages generated by the Application Firewall.

field consistency (fieldconLog) Number of Field Consistency security check log messages generated by the Application Firewall.

credit cards (ccardLog) Number of Credit Card security check log messages generated by the Application Firewall.

safe object logs (safeobjLog) Number of Safe Object security check log messages generated by the Application Firewall.

Signature logs (sigsLog) Number of Signature logs generated by the Application Firewall.

content Type logs (contentTypeLog) Number of content type security check log messages generated by the Application Firewall.

JSON Denial of Service logs (jsondosLogs) Number of JSON Denial-of-Service security check log messages generated by the Application Firewall.

JSON SQL injection logs (jsonsqlLogs) Number of JSON SQL Injection security check log messages generated by the Application Firewall.

JSON Cross-Site Scripting logs (jsonxssLogs) Number of JSON Cross-Site Scripting (XSS) security check log messages generated by the Application Firewall.

JSON CMD injection logs (jsoncmdLogs) Number of JSON Command Injection security check log messages generated by the Application Firewall.

file upload types logs (fileUploadTypesLog) Number of File Upload Types security check log messages generated by the Application Firewall.

Infer Content Type XML Payload Logs (inferContentTypeLog) Number of Mismatched Content-Type in request with XML Payload security check logs seen by the Application Firewall.

HTML Command Injection logs (cmdLog) Number of HTML Command Injection security check log messages generated by the Application Firewall.

XML Format logs (wfcLogs) Number of XML Format security check log messages generated by the Application Firewall.

XML Denial of Service (XDoS) log messages (xdosLogs) Number of XML Denial-of-Service security check log messages generated by the Application Firewall.

XML Message Validation logs (msgvalLogs) Number of XML Message Validation security check log messages generated by the Application Firewall.

WSI logs (wsiLogs) Number of Web Services Interoperability (WS-I) security check log messages generated by the Application Firewall.

XML SQL Injection logs (xmlSqlLogs) Number of XML SQL Injection security check log messages generated by the Application Firewall.

XML XSS logs (xmlXssLogs) Number of XML Cross-Site Scripting (XSS) security check log messages generated by the Application Firewall.

XML Attachment logs (xmlAttachmentLogs) Number of XML Attachment security check log messages generated by the Application Firewall.

SOAP Fault logs (soapfltLog) Number of requests generating soap:fault log messages

XML Generic logs (genfltLog) Number of requests generating XML generic error log messages

HTML SQL logs (SQL grammar) (sqlGramLog) Number of HTML SQL Injection security check log messages (reported by SQL grammar) generated by the Application Firewall.

JSON SQL injection logs (SQL grammar) (jsonsqlGramLogs) Number of JSON SQL Injection security check log messages (reported by SQL grammar) generated by the Application Firewall.

HTML CMD logs (CMD grammar) (cmdGramLog) Number of HTML CMD Injection security check log messages (reported by CMD grammar) generated by the Application Firewall.

JSON CMD injection logs (CMD grammar) (jsoncmdGramLogs) Number of JSON CMD Injection security check log messages (reported by CMD grammar) generated by the Application Firewall.

HTML Block Keyword logs (blockKeywordLog) Number of HTML Block Keyword security check log messages generated by the Application Firewall.

JSON Block Keyword logs (JSONblockKeywordLog) Number of JSON Block Keyword security check log messages generated by the Application Firewall.

HTTP Client Errors (4xx Resp) (4xxResps) Number of requests returning HTTP 4xx from the backend server

HTTP Server Errors (5xx Resp) (5xxResps) Number of requests returning HTTP 5xx from the backend server

Config Start URL Closure (cfgstarturlclosure) Number of profiles with Start URL Closure enabled in the Application Firewall.

Config Cookie Transforms (cfgcookietransforms) Number of profiles with Config Cookie Transforms enabled in the Application Firewall.

Config CrossSite Scripting Transform Unsafe HTML (cfgcrosssitescriptingtransformunsafehtml) Number of profiles with CrossSite Scripting Transform Unsafe HTML enabled in the Application Firewall.

Config CrossSite Scripting Check Complete URLs (cfgcrosssitescriptingcheckcompleteurls) Number of profiles with CrossSite Scripting Check Complete URLs enabled in the Application Firewall.

Config SQL Injection Grammar (cfgsqlinjectiongrammar) Number of profiles with SQL Injection Grammar enabled in the Application Firewall.

Config SQL Injection Transform Special Characters (cfgsqlinjectiontransformspecialchars) Number of profiles with SQL Injection Transform Special Characters enabled in the Application Firewall.

Config SQL Injection Check SQL Wild Characters (cfgsqlinjectionchecksqlwildchars) Number of profiles with SQL Injection Check SQL Wild Characters enabled in the Application Firewall.

Config Credit Card XOut (cfgcreditcardxout) Number of profiles with Credit Card XOut enabled in the Application Firewall.

Config Do Secure Credit Card Logging (cfgdosecurecreditcardlogging) Number of profiles with Do Secure Credit Card Logging enabled in the Application Firewall.

Config Streaming (cfgstreaming) Number of profiles with Streaming enabled in the Application Firewall.

Config Trace (cfgtrace) Number of profiles with Trace enabled in the Application Firewall.

Config JSON SQL Injection Grammar (cfgjsonsqlinjectiongrammar) Number of profiles with JSON SQL Injection Grammar enabled in the Application Firewall.

Config XML SQL Injection Check SQL Wild Chars (cfgxmlsqlinjectionchecksqlwildchars) Number of profiles with XML SQL Injection Check SQL Wild Chars enabled in the Application Firewall.

Config Use HTML Error Object (cfgusehtmlerrorobject) Number of profiles with Use HTML Error Object enabled in the Application Firewall.

Config Log Every Policy Hit (cfglogeverypolicyhit) Number of profiles with Log Every Policy Hit enabled in the Application Firewall.

Config Exempt Closure URLs From Security Checks (cfgexemptclosureurlsfromsecuritychecks) Number of profiles with Exempt Closure URLs From Security Checks enabled in the Application Firewall.

Config Canonicalize HTML Response (cfgcanonicalizehtmlresponse) Number of profiles with Canonicalize HTML Response enabled in the Application Firewall.

Config Enable Form Tagging (cfgenableformtagging) Number of profiles with Enable Form Tagging enabled in the Application Firewall.

Config Sessionless URL Closure (cfgsessionless_url_closure) Number of profiles with Sessionless URL Closure enabled in the Application Firewall.

Config Semicolon Field Separator (cfgsemicolonfieldseparator) Number of profiles with Semicolon Field Separator enabled in the Application Firewall.

Config Exclude File Upload From Checks (cfgexcludefileuploadfromchecks) Number of profiles with Exclude File Upload From Checks enabled in the Application Firewall.

Config Check Request Headers (cfgcheckrequestheaders) Number of profiles with Check Request Headers enabled in the Application Firewall.

Config Optimize Partial Reqs (cfgoptimizepartialreqs) Number of profiles with Optimize Partial Reqs enabled in the Application Firewall.

Config URL Decode Request Cookies (cfgurldecoderequestcookies) Number of profiles with URL Decode Request Cookies enabled in the Application Firewall.

Config Percent Decode Recursively (cfgpercentdecoderecursively) Number of profiles with Percent Decode Recursively enabled in the Application Firewall.

Config Insert Cookie SameSite Attribute (cfginsertcookiesamesiteattribute) Number of profiles with Insert Cookie SameSite Attribute enabled in the Application Firewall.

Config Fake Account Detection (cfgfakeaccountdetection) Number of profiles with Fake Account Detection enabled in the Application Firewall.

credit card log transform messages (ccardXformLog) Number of Credit Card security check transform log messages generated by the Application Firewall.

Related Commands

- stat appfw policylabel

appqoe

appqoe-CustomResp

The following operations can be performed on "appqoe-CustomResp":

rm| show| update| import|

rm appqoe CustomResp

Removes the imported HTML object.

Synopsis

rm appqoe CustomResp <name>

Arguments

name Indicates name of the custom response HTML page to import/update.

Example

rm appqoe CustomResp appqoe_resp

show appqoe CustomResp

Displays lists all HTML page objects on the Citrix ADC.

Synopsis

show appqoe CustomResp

Arguments

Output

name Indicates name of the custom response HTML page to import/update.

src devno count stateflag

Example

show appqoe CustomResp

update appqoe CustomResp

Update the imported HTML object

Synopsis

update appqoe CustomResp <name>

Arguments

name Indicates name of the custom response HTML page to import/update.

Example

update appqoe CustomResp appqoe_resp

import appqoe CustomResp

Downloads the input HTML Page to Citrix ADC Box with the given object name

Synopsis

import appqoe CustomResp <name>

Arguments

src name Indicates name of the custom response HTML page to import/update.

Example

import appqoe CustomResp http://10.102.34.25/index.html appqoe_resp

appqoe-action

The following operations can be performed on "appqoe-action":

add| rm| set| show| unset|

add appqoe action

Add a new AppQoE action for triggering

Synopsis

add appqoe action <name> [-respondWith (ACS | NS)] [-retryOnReset (YES | NO)]

Arguments

name Name for the AppQoE action. Must begin with a letter, number, or the underscore symbol (_). Other characters allowed, after the first character, are the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), and colon (:) characters. This is a mandatory argument

priority Priority for queuing the request. If server resources are not available for a request that matches the configured rule, this option specifies a priority for queuing the request until the server resources are available again. If priority is not configured then Lowest priority will be used to queue the request.

Possible values: HIGH, MEDIUM, LOW, LOWEST

respondWith Responder action to be taken when the threshold is reached. Available settings function as follows: ACS - Serve content from an alternative content service Threshold : maxConn or delay NS - Serve from the Citrix ADC (built-in response) Threshold : maxConn or delay

Possible values: ACS, NS

CustomFile name of the HTML page object to use as the response

altContentSvcName Name of the alternative content service to be used in the ACS

altContentPath Path to the alternative content service to be used in the ACS

polqDepth Policy queue depth threshold value. When the policy queue size (number of requests queued for the policy binding this action is attached to) increases to the specified polqDepth value, subsequent requests are dropped to the lowest priority level. Minimum value: 0 Maximum value: 4294967294

priqDepth Queue depth threshold value per priorirty level. If the queue size (number of requests in the queue of that particular priorirty) on the virtual server to which this policy is bound, increases to the specified qDepth value, subsequent requests are dropped to the lowest priority level. Minimum value: 0 Maximum value: 4294967294

maxConn Maximum number of concurrent connections that can be open for requests that matches with rule. Minimum value: 1 Maximum value: 4294967294

delay Delay threshold, in microseconds, for requests that match the policy's rule. If the delay statistics gathered for the matching request exceed the specified delay, configured action triggered for that request, if there is no action then requests are dropped to the lowest priority level Minimum value: 1 Maximum value: 599999999

dosTrigExpression Optional expression to add second level check to trigger DoS actions. Specifically used for Analytics based DoS response generation

dosAction DoS Action to take when vserver will be considered under DoS attack and corresponding rule matches. Mandatory if AppQoE actions are to be used for DoS attack prevention.

Possible values: SimpleResponse, HICResponse

tcpprofile Bind TCP Profile based on L2/L3/L7 parameters.

retryOnReset Retry on TCP Reset

Possible values: YES, NO Default value: NO

retryOnTimeout Retry on request Timeout(in millisec) upon sending request to backend servers Minimum value: 30 Maximum value: 2000

numretries Retry count Default value: 3 Minimum value: 0 Maximum value: 7

rm appqoe action

Removes the specified AppQoE action.

Synopsis

rm appqoe action <name>

Arguments

name Name of the action to be removed.

set appqoe action

Set the argument of specified AppQoE action.

Synopsis

set appqoe action <name>

Arguments

name Name for the AppQoE action. Must begin with a letter, number, or the underscore symbol (_). Other characters allowed, after the first character, are the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), and colon (:) characters. This is a mandatory argument

priority Priority for queuing the request. If server resources are not available for a request that matches the configured rule, this option specifies a priority for queuing the request until the server resources are available again. If priority is not configured then Lowest priority will be used to queue the request.

Possible values: HIGH, MEDIUM, LOW, LOWEST

altContentSvcName Name of the alternative content service to be used in the ACS

altContentPath Path to the alternative content service to be used in the ACS

polqDepth Policy queue depth threshold value. When the policy queue size (number of requests queued for the policy binding this action is attached to) increases to the specified polqDepth value, subsequent requests are dropped to the lowest priority level. Minimum value: 0 Maximum value: 4294967294

priqDepth Queue depth threshold value per priorirty level. If the queue size (number of requests in the queue of that particular priorirty) on the virtual server to which this policy is bound, increases to the specified qDepth value, subsequent requests are dropped to the lowest priority level. Minimum value: 0 Maximum value: 4294967294

maxConn Maximum number of concurrent connections that can be open for requests that matches with rule. Minimum value: 1 Maximum value: 4294967294

delay Delay threshold, in microseconds, for requests that match the policy's rule. If the delay statistics gathered for the matching request exceed the specified delay, configured action triggered for that request, if there is no action then requests are dropped to the lowest priority level Minimum value: 1 Maximum value: 599999999

dosTrigExpression Optional expression to add second level check to trigger DoS actions. Specifically used for Analytics based DoS response generation

dosAction DoS Action to take when vserver will be considered under DoS attack and corresponding rule matches. Mandatory if AppQoE actions are to be used for DoS attack prevention.

Possible values: SimpleResponse, HICResponse

tcpprofile Bind TCP Profile based on L2/L3/L7 parameters.

retryOnReset Retry on TCP Reset

Possible values: YES, NO Default value: NO

retryOnTimeout Retry on request Timeout(in millisec) upon sending request to backend servers Minimum value: 30 Maximum value: 2000

numretries Retry count Default value: 3 Minimum value: 0 Maximum value: 7

show appqoe action

Display configured AppQoE action(s).

Synopsis

show appqoe action

Arguments

name Name for the AppQoE action. Must begin with a letter, number, or the underscore symbol (_). Other characters allowed, after the first character, are the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), and colon (:) characters. This is a mandatory argument

Output

stateflag hits priority Priority for queuing the request. If server resources are not available for a request that matches the configured rule, this option specifies a priority for queuing the request until the server resources are available again. If priority is not configured then Lowest priority will be used to queue the request.

respondWith Responder action to be taken when the threshold is reached. Available settings function as follows: ACS - Serve content from an alternative content service Threshold : maxConn or delay NS - Serve from the Citrix ADC (built-in response) Threshold : maxConn or delay

polqDepth Policy queue depth threshold value. When the policy queue size (number of requests queued for the policy binding this action is attached to) increases to the specified polqDepth value, subsequent requests are dropped to the lowest priority level.

priqDepth Queue depth threshold value per priorirty level. If the queue size (number of requests in the queue of that particular priorirty) on the virtual server to which this policy is bound, increases to the specified qDepth value, subsequent requests are dropped to the lowest priority level.

altContentSvcName Name of the alternative content service to be used in the ACS

altContentPath Path to the alternative content service to be used in the ACS

maxConn Maximum number of concurrent connections that can be open for requests that matches with rule.

delay Delay threshold, in microseconds, for requests that match the policy's rule. If the delay statistics gathered for the matching request exceed the specified delay, configured action triggered for that request, if there is no action then requests are dropped to the lowest priority level

CustomFile name of the HTML page object to use as the response

dosTrigExpression Optional expression to add second level check to trigger DoS actions. Specifically used for Analytics based DoS response generation

dosAction DoS Action to take when vserver will be considered under DoS attack and corresponding rule matches. Mandatory if AppQoE actions are to be used for DoS attack prevention.

tcpprofile Bind TCP Profile based on L2/L3/L7 parameters.

retryOnReset Retry on TCP Reset

retryOnTimeout Retry on request Timeout(in millisec) upon sending request to backend servers

numretries Retry count

devno count

unset appqoe action

Use this command to remove appqoe action settings.Refer to the set appqoe action command for meanings of the arguments.

Synopsis

unset appqoe action <name>

Appqoe

The entities on which you can perform NetScaler CLI operations:

- appqoe-CustomResp

- appqoe-action
- appqoe
- appqoe-parameter
- appqoe-policy
- appqoe-stats

appqoe-parameter

The following operations can be performed on "appqoe-parameter":

show| set| unset|

show appqoe parameter

Displays the values of the session life and filename parameters

Synopsis

show appqoe parameter

Arguments

Output

sessionLife appqoe session life (in seconds)

avgwaitingclient average number of client connections, that can sit in service waiting queue

MaxAltRespBandWidth maximum bandwidth which will determine whether to send alternate content response

dosAttackThresh average number of client connection that can queue up on vserver level without triggering DoS mitigation module

Example

show appqos parameter

set appqoe parameter

Sets the parameters for displaying appqoe information.

Synopsis

set appqoe parameter

Arguments

sessionLife Time, in seconds, between the first time and the next time the AppQoE alternative content window is displayed. The alternative content window is displayed only once during a session for the same browser accessing a configured URL, so this parameter determines the length of a session. Default value: 300 Minimum value: 1 Maximum value: 4294967294

avgwaitingclient average number of client connections, that can sit in service waiting queue Default value: 1000000 Minimum value: 0 Maximum value: 4294967294

MaxAltRespBandWidth maximum bandwidth which will determine whether to send alternate content response Default value: 100 Minimum value: 1 Maximum value: 4294967294

dosAttackThresh average number of client connection that can queue up on vserver level without triggering DoS mitigation module Default value: 2000 Minimum value: 0 Maximum value: 4294967294

Example

set appqoe parameter -sessionlife 200 -avgwaitingclient 10

unset appqoe parameter

Use this command to remove appqoe parameter settings.Refer to the set appqoe parameter command for meanings of the arguments.

Synopsis

unset appqoe parameter

appqoe-policy

The following operations can be performed on "appqoe-policy":

set| show| add| rm| stat|

set appqoe policy

Synopsis

set appqoe policy <name>

Arguments

name rule Expression or name of a named expression, against which the request is evaluated. The policy is applied if the rule evaluates to true.

action Configured AppQoE action to trigger

show appqoe policy

Display all the configured AppQoE policies.

Synopsis

show appqoe policy

Arguments

name

Output

stateflag rule Expression or name of a named expression, against which the request is evaluated. The policy is applied if the rule evaluates to true.

action Configured AppQoE action to trigger

hits Number of hits.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

bindPriority Specifies the binding of the policy. use only in display

boundTo The name of the entity to which the policy is bound.

activePolicy type devno count

add appqoe policy

Add a new AppQoE policy for binding rule with action

Synopsis

add appqoe policy <name> -rule <expression> -action <string>

Arguments

name rule Expression or name of a named expression, against which the request is evaluated. The policy is applied if the rule evaluates to true.

action Configured AppQoE action to trigger

rm appqoe policy

Remove an AppQoE policy.

Synopsis

rm appqoe policy <name>

Arguments

name Name of the AppQoE policy to be removed.

stat appqoe policy

Displays collected brief statistics for all AppQoE policies, or detailed statistics for only the specified policy.

Synopsis

stat appqoe policy

Arguments

name policyName

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Server TTFB (SvrTTFB) Server Time-To-First-Byte in milliseconds calculated for this AppQoE policy.

Server TTFB (SvrTTFB) Server Time-To-First-Byte in milliseconds calculated for this AppQoE policy.

Server TTLB (SvrTTLB) Server Time-To-Last-Byte in milliseconds calculated for this AppQoE policy.

Server TTLB (SvrTTLB) Server Time-To-Last-Byte in milliseconds calculated for this AppQoE policy.

Client TTLB (CltTTLB) Client Time-To-Last-Byte in milliseconds calculated for this AppQoE policy.

Client TTLB (CltTTLB) Client Time-To-Last-Byte in milliseconds calculated for this AppQoE policy.

Average Server TTFB (SvrTTFB) Average Server Time-To-First-Byte in milliseconds calculated for this AppQoE policy.

Average Server TTLB (SvrTTLB) Average Server Time-To-Last-Byte in milliseconds calculated for this AppQoE policy.

Average Client TTLB (CltTTLB) Average Client Time-To-Last-Byte in milliseconds calculated for this AppQoE policy.

ThroughPut(Kbps) (ThroughPut) Throughput in Kbps calculated on this AppQoE policy

Server TCP connections (TotSvr) Total number of server connections that were established through this AppQoE Policy

Client TCP connections (TotClt) Total number of client connections that were requested through this AppQoE Policy

Requests received (TotReq) Total number of requests that were requested through this AppQoE policy

Requests bytes (TotReqBytes) Total number of requests bytes that were requested through this AppQoE policy

Responses received (TotRsp) Total number of responses received by this AppQoE policy

Response bytes (TotRspBytes) Total number of response bytes received by this AppQoE policy

Alternate responses sent (TotJSsent) Total number of in-memory responses sent instead of expected responses through this AppQoE policy

Alternate responses bytes sent (TotJSBytessent) Total bytes of in-memory responses sent through this AppQoE policy

Policy hits (Hits) Number of hits on the policy

Client HTTP transactions Total number of client transactions processed by this AppQoE policy.

Svr HTTP transactions Total number of server transactions processed by this AppQoE policy.

Svr HTTP transactions Total number of server transactions processed by this AppQoE policy.

Client TTLB (CltTTLB) Client Time-To-Last-Byte in milliseconds calculated for this AppQoE policy.

Server TTLB (SvrTTLB) Server Time-To-Last-Byte in milliseconds calculated for this AppQoE policy.

Server TTFB (SvrTTFB) Server Time-To-First-Byte in milliseconds calculated for this AppQoE policy.

Example

stat appqos policy

appqoe-stats

The following operations can be performed on "appqoe-stats":

show appqoe stats

show appqoe stats is an alias for stat appqoe Displays global AppQoE statistics.

Synopsis

show appqoe stats - alias for 'stat appqoe'

appqoe

The following operations can be performed on "appqoe":

stat appqoe

Displays statistics of feature AppQoE.

Synopsis

stat appqoe

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

In-Memory responses sent (TotInMemRsp) Total in-memory responses sent from NS

Faulty cookies received (TotFaultyCookies) Total faulty cookies received

Valid cookies received (TotValidCookies) Total valid cookies received

High priority requests served (TotHighPriReq) Total Requests served from higher priority queue

Medium priority requests served (TotMediumPriReq) Total Requests served from medium priority queue

Low priority requests served (TotLowPriReq) Total Requests served from low priority queue

Lowest(Surge) priority requests served (TotLowestPriReq) Total Requests served from surge priority queue

Alt. server substitution failed (TotAltSvrSubFailed) Total number of times alternate server substitution failed

HDOS condition triggered (TotDoSTrig) Total number of times HDOS condition triggered

Valid DOSQ cookies received (TotDOSQValidCookies) Total DOSQ valid cookies received

Valid DOSH cookies received (TotDOSHValidCookies) Total DOSH valid cookies received

Valid SID cookies received (TotSIDValidCookies) Total SID valid cookies received

Valid ONH cookies received (TotONHValidCookies) Total ONH valid cookies received

Valid PRIQ cookies received (TotPRIQValidCookies) Total PRIQ valid cookies received

Faulty DOSQ cookies received (TotDOSQFaultyCookies) Total DOSQ faulty cookies received

Faulty DOSH cookies received (TotDOSHFaultyCookies) Total DOSH faulty cookies received

Faulty SID cookies received (TotSIDFaultyCookies) Total SID faulty cookies received

Faulty ONH cookies received (TotONHFaultyCookies) Total ONH faulty cookies received

Faulty PRIQ cookies received (TotPRIQFaultyCookies) Total PRIQ faulty cookies received

Requests for valid embedded links (TotPRIEmbedLinks) Total requests for valid embedded links

Valid SIDQ req. within session (TotSessReq) Total valid SIDQ requests within session

Requests for alternate contents (TotAltCntReq) Total requests for alternate contents

In-Memory GET responses sent (TotGETInMemRsp) Total in-memory GET responses sent from NS

In-Memory POST responses sent (TotPOSTInMemRsp) Total in-memory POST responses sent from NS

In-Memory response bytes sent (TotInMemRspbytes) Total in-memory response bytes sent from NS

Related Commands

- stat appqoe policy

audit

Audit

The entities on which you can perform NetScaler CLI operations:

- audit
- audit-messageaction
- audit-messages
- audit-nslogAction
- audit-nslogGlobal
- audit-nslogParams
- audit-nslogPolicy
- audit-stats
- audit-syslogAction
- audit-syslogGlobal
- audit-syslogParams
- audit-syslogPolicy

audit-messageaction

The following operations can be performed on "audit-messageaction":

add| set| rm| show| unset|

add audit messageaction

Adds an audit message action. The action specifies whether to log the message, and to which log.

Synopsis

add audit messageaction <name> <logLevel> <stringBuilderExpr>

Arguments

name Name of the audit message action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the message action is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my message action" or 'my message action').

logLevel Audit log level, which specifies the severity level of the log message being generated.. The following loglevels are valid:

- EMERGENCY - Events that indicate an immediate crisis on the server.
- ALERT - Events that might require action.
- CRITICAL - Events that indicate an imminent server crisis.
- ERROR - Events that indicate some type of error.
- WARNING - Events that require action in the near future.
- NOTICE - Events that the administrator should know about.
- INFORMATIONAL - All but low-level events.
- DEBUG - All events, in extreme detail.

Possible values: EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG

stringBuilderExpr Default-syntax expression that defines the format and content of the log message.

logtoNewnslog Send the message to the new nslog.

Possible values: YES, NO

set audit messageaction

Modifies the specified parameters of an existing audit message action.

Synopsis

set audit messageaction <name>

Arguments

name Name of the audit message action to modify.

logLevel Audit log level, which specifies the severity level of the log message being generated. The following loglevels are valid:

- EMERGENCY - Events that indicate an immediate crisis on the server.
- ALERT - Events that might require action.
- CRITICAL - Events that indicate an imminent server crisis.
- ERROR - Events that indicate some type of error.
- WARNING - Events that require action in the near future.
- NOTICE - Events that the administrator should know about.
- INFORMATIONAL - All but low-level events.
- DEBUG - All events, in extreme detail.

Possible values: EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG

stringBuilderExpr Default-syntax expression that defines the format and content of the log message.

logtoNewnslog Send the message to the new nslog.

Possible values: YES, NO

rm audit messageaction

Removes the specified audit message action and associated configuration.

Synopsis

rm audit messageaction <name>

Arguments

name Name of the audit message action to remove.

show audit messageaction

Displays the current configuration of the specified audit message action. If no audit message action is specified, displays a list of all audit message actions currently configured on the Citrix ADC.

Synopsis

show audit messageaction

Arguments

name Name of the audit message action.

Output

logLevel Audit log level, which specifies the severity level of the log message being generated.. The following loglevels are valid:

- EMERGENCY - Events that indicate an immediate crisis on the server.
- ALERT - Events that might require action.
- CRITICAL - Events that indicate an imminent server crisis.
- ERROR - Events that indicate some type of error.
- WARNING - Events that require action in the near future.
- NOTICE - Events that the administrator should know about.
- INFORMATIONAL - All but low-level events.
- DEBUG - All events, in extreme detail.

logLevel stringBuilderExpr Default-syntax expression that defines the format and content of the log message.

logtoNewnslog Send the message to the new nslog.

bypassSafetyCheck Bypass the safety check and allow unsafe expressions.

stateflag hits The number of times the action has been taken.

undefHits The number of times the action resulted in UNDEF.

referenceCount The number of references to the action.

gslbBindings Number of times action is used in a policy bound to a gslb vserver

devno count

unset audit messageaction

Use this command to remove audit messageaction settings.Refer to the set audit messageaction command for meanings of the arguments.

Synopsis

unset audit messageaction <name> -logtoNewnslog

audit-messages

The following operations can be performed on "audit-messages":

show audit messages

Displays the most recent audit log messages.

Synopsis

show audit messages

Arguments

logLevel Audit log level filter, which specifies the types of events to display. The following loglevels are valid:

- ALL - All events.
- EMERGENCY - Events that indicate an immediate crisis on the server.
- ALERT - Events that might require action.
- CRITICAL - Events that indicate an imminent server crisis.
- ERROR - Events that indicate some type of error.
- WARNING - Events that require action in the near future.
- NOTICE - Events that the administrator should know about.
- INFORMATIONAL - All but low-level events.
- DEBUG - All events, in extreme detail.

numOfMesgs Number of log messages to be displayed. Default value: 20 Minimum value: 1 Maximum value: 256

Output

value The Audit message

devno count stateflag

audit-nslogAction

The following operations can be performed on "audit-nslogAction":

set| add| rm| show| unset|

set audit nslogAction

Modifies the specified settings of an existing nslog action.

Synopsis

set audit nslogAction <name>

Arguments

name Name of the nslog action to be modified.

serverIP IP address of the nslog server.

serverDomainName Auditserver name as a FQDN. Mutually exclusive with serverIP

domainResolveRetry Time, in seconds, for which the Citrix ADC waits before sending another DNS query to resolve the host name of the audit server if the last query failed. Default value: 5 Minimum value: 5 Maximum value: 20939

domainResolveNow Immediately send a DNS query to resolve the server's domain name.

serverPort Port on which the nslog server accepts connections. Minimum value: 1

logLevel Audit log level, which specifies the types of events to log. Available settings function as follows:

- ALL - All events.
- EMERGENCY - Events that indicate an immediate crisis on the server.
- ALERT - Events that might require action.
- CRITICAL - Events that indicate an imminent server crisis.
- ERROR - Events that indicate some type of error.
- WARNING - Events that require action in the near future.
- NOTICE - Events that the administrator should know about.
- INFORMATIONAL - All but low-level events.
- DEBUG - All events, in extreme detail.

- NONE - No events.

dateFormat Format of dates in the logs. Supported formats are:

- MMDDYYYY - U.S. style month/date/year format.
- DDMMYYYY - European style date/month/year format.
- YYYYMMDD - ISO style year/month/date format.

Possible values: MMDDYYYY, DDMMYYYY, YYYYMMDD

logFacility Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the Citrix ADC itself, the VPN, or external.

Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7

tcp Log TCP messages.

Possible values: NONE, ALL

acl Log access control list (ACL) messages.

Possible values: ENABLED, DISABLED

timeZone Time zone used for date and timestamps in the logs. Available settings function as follows:

- GMT_TIME. Coordinated Universal Time.
- LOCAL_TIME. The server's timezone setting.

Possible values: GMT_TIME, LOCAL_TIME

userDefinedAuditlog Log user-configurable log messages to nslog. Setting this parameter to NO causes auditing to ignore all user-configured message actions. Setting this parameter to YES causes auditing to log user-configured message actions that meet the other logging criteria.

Possible values: YES, NO

appflowExport Export log messages to AppFlow collectors. Appflow collectors are entities to which log messages can be sent so that some action can be performed on them.

Possible values: ENABLED, DISABLED

lsn Log the LSN messages

Possible values: ENABLED, DISABLED

alg Log the ALG messages

Possible values: ENABLED, DISABLED

subscriberLog Log subscriber session event information

Possible values: ENABLED, DISABLED

sslInterception Log SSL Interception event information

Possible values: ENABLED, DISABLED

urlFiltering Log URL filtering event information

Possible values: ENABLED, DISABLED

ContentInspectionLog Log Content Inspection event information

Possible values: ENABLED, DISABLED

add audit nslogAction

Adds an nslog action. The action contains a reference to an nslog server and specifies which information to log and how to log that information.

Synopsis

add audit nslogAction <name> (<serverIP> | (<serverDomainName>)) -logLevel <logLevel> ...

Arguments

name Name of the nslog action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the nslog action is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my nslog action" or 'my nslog action').

serverIP IP address of the nslog server.

serverDomainName Auditserver name as a FQDN. Mutually exclusive with serverIP

domainResolveRetry Time, in seconds, for which the Citrix ADC waits before sending another DNS query to resolve the host name of the audit server if the last query failed. Default value: 5 Minimum value: 5 Maximum value: 20939

serverPort Port on which the nslog server accepts connections. Minimum value: 1

logLevel Audit log level, which specifies the types of events to log. Available settings function as follows:

- ALL - All events.
- EMERGENCY - Events that indicate an immediate crisis on the server.
- ALERT - Events that might require action.
- CRITICAL - Events that indicate an imminent server crisis.
- ERROR - Events that indicate some type of error.
- WARNING - Events that require action in the near future.
- NOTICE - Events that the administrator should know about.
- INFORMATIONAL - All but low-level events.
- DEBUG - All events, in extreme detail.
- NONE - No events.

dateFormat Format of dates in the logs. Supported formats are:

- MMDDYYYY - U.S. style month/date/year format.
- DDMMYYYY - European style date/month/year format.
- YYYYMMDD - ISO style year/month/date format.

Possible values: MMDDYYYY, DDMMYYYY, YYYYMMDD

logFacility Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the Citrix ADC itself, the VPN, or external.

Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7

tcp Log TCP messages.

Possible values: NONE, ALL

acl Log access control list (ACL) messages.

Possible values: ENABLED, DISABLED

timeZone Time zone used for date and timestamps in the logs. Available settings function as follows:

- GMT_TIME. Coordinated Universal Time.
- LOCAL_TIME. The server's timezone setting.

Possible values: GMT_TIME, LOCAL_TIME

userDefinedAuditlog Log user-configurable log messages to nslog. Setting this parameter to NO causes auditing to ignore all user-configured message actions. Setting this parameter to YES causes auditing to log user-configured message actions that meet the other logging criteria.

Possible values: YES, NO

appflowExport Export log messages to AppFlow collectors. Appflow collectors are entities to which log messages can be sent so that some action can be performed on them.

Possible values: ENABLED, DISABLED

lsn Log the LSN messages

Possible values: ENABLED, DISABLED

alg Log the ALG messages

Possible values: ENABLED, DISABLED

subscriberLog Log subscriber session event information

Possible values: ENABLED, DISABLED

sslInterception Log SSL Interception event information

Possible values: ENABLED, DISABLED

urlFiltering Log URL filtering event information

Possible values: ENABLED, DISABLED

ContentInspectionLog Log Content Inspection event information

Possible values: ENABLED, DISABLED

rm audit nslogAction

Removes the specified nslog action and associated configuration. Note: An nslog action cannot be removed if it is bound to an nslog policy.

Synopsis

rm audit nslogAction <name>

Arguments

name Name of the nslog action to remove.

show audit nslogAction

Displays the current configuration of the specified nslog action. If no nslog action is specified, displays a list of all nslog actions currently configured on the Citrix ADC.

Synopsis

show audit nslogAction

Arguments

name Name of the nslog action.

Output

serverIP IP address of the nslog server.

serverDomainName Auditserver name as a FQDN. Mutually exclusive with serverIP

domainResolveRetry Time, in seconds, for which the Citrix ADC waits before sending another DNS query to resolve the host name of the audit server if the last query failed.

domainResolveNow Immediately send a DNS query to resolve the server's domain name.

IP The resolved IP address of the auditserver

serverPort Port on which the nslog server accepts connections.

logLevel Audit log level, which specifies the types of events to log. Available settings function as follows:

- ALL - All events.
- EMERGENCY - Events that indicate an immediate crisis on the server.

- ALERT - Events that might require action.
- CRITICAL - Events that indicate an imminent server crisis.
- ERROR - Events that indicate some type of error.
- WARNING - Events that require action in the near future.
- NOTICE - Events that the administrator should know about.
- INFORMATIONAL - All but low-level events.
- DEBUG - All events, in extreme detail.
- NONE - No events.

dateFormat Format of dates in the logs. Supported formats are:

- MMDDYYYY - U.S. style month/date/year format.
- DDMMYYYY - European style date/month/year format.
- YYYYMMDD - ISO style year/month/date format.

logFacility Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the Citrix ADC itself, the VPN, or external.

tcp Log TCP messages.

acl Log access control list (ACL) messages.

timeZone Time zone used for date and timestamps in the logs. Available settings function as follows:

- GMT_TIME. Coordinated Universal Time.
- LOCAL_TIME. The server's timezone setting.

stateflag userDefinedAuditlog Log user-configurable log messages to nslog. Setting this parameter to NO causes auditing to ignore all user-configured message actions. Setting this parameter to YES causes auditing to log user-configured message actions that meet the other logging criteria.

appflowExport Export log messages to AppFlow collectors. Appflow collectors are entities to which log messages can be sent so that some action can be performed on them.

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

lsn Log the LSN messages

alg Log the ALG messages

subscriberLog Log subscriber session event information

sslInterception Log SSL Interception event information

urlFiltering Log URL filtering event information

ContentInspectionLog Log Content Inspection event information

devno count

unset audit nslogAction

Removes the settings of an existing nslog action. Attributes for which a default value is available revert to their default values. See the set audit nslogAction command for descriptions of the parameters..Refer to the set audit nslogAction command for meanings of the arguments.

Synopsis

unset audit nslogAction <name>

audit-nslogGlobal

The following operations can be performed on "audit-nslogGlobal":

bind| unbind| show|

bind audit nslogGlobal

binds audit nslog policy to audit nslogGlobal

Synopsis

bind audit nslogGlobal -policyName <string> -priority <positive_integer>

Arguments

policyName Name of the audit nslog policy.

priority Specifies the priority of the policy. Minimum value: 1 Maximum value: 2147483647

globalBindType

Example

bind audit nslogGlobal -policyname pol9 -priority 9

unbind audit nslogGlobal

Unbind the specified audit nslog policy from audit nslogGlobal.

Synopsis

unbind audit nslogGlobal

Arguments

policyName Name of the policy to unbind.

globalBindType

Example

unbind audit nslogGlobal pol9

show audit nslogGlobal

Displays the list of policies bound to audit nslogGlobal bind point.

Synopsis

show audit nslogGlobal

Arguments

Output

stateflag policyName Name of the audit nslog policy.

priority Specifies the priority of the policy.

numpol number of polices bound to label.

flags globalBindType type The bindpoint to which the policy is bound

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

devno count

Example

show audit nslogGlobal

audit-nslogParams

The following operations can be performed on "audit-nslogParams":

set| unset| show|

set audit nslogParams

Modifies the specified nslog parameters. Changes the IP address, the port, or the logging parameters for logs sent to nslog.

Synopsis

set audit nslogParams

Arguments

serverIP IP address of the nslog server.

serverPort Port on which the nslog server accepts connections. Minimum value: 1

dateFormat Format of dates in the logs. Supported formats are:

- MMDDYYYY - U.S. style month/date/year format.
- DDMMYYYY - European style date/month/year format.
- YYYYMMDD - ISO style year/month/date format.

Possible values: MMDDYYYY, DDMMYYYY, YYYYMMDD

logLevel Types of information to be logged. Available settings function as follows:

- ALL - All events.
- EMERGENCY - Events that indicate an immediate crisis on the server.
- ALERT - Events that might require action.
- CRITICAL - Events that indicate an imminent server crisis.
- ERROR - Events that indicate some type of error.
- WARNING - Events that require action in the near future.
- NOTICE - Events that the administrator should know about.

- INFORMATIONAL - All but low-level events.
- DEBUG - All events, in extreme detail.
- NONE - No events.

logFacility Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the Citrix ADC itself, the VPN, or external.

Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7

tcp Configure auditing to log TCP messages.

Possible values: NONE, ALL

acl Configure auditing to log access control list (ACL) messages.

Possible values: ENABLED, DISABLED

timeZone Time zone used for date and timestamps in the logs. Supported settings are:

- GMT_TIME - Coordinated Universal Time.
- LOCAL_TIME - Use the server's timezone setting.

Possible values: GMT_TIME, LOCAL_TIME

userDefinedAuditlog Log user-configurable log messages to nslog. Setting this parameter to NO causes auditing to ignore all user-configured message actions. Setting this parameter to YES causes auditing to log user-configured message actions that meet the other logging criteria.

Possible values: YES, NO

appflowExport Export log messages to AppFlow collectors. Appflow collectors are entities to which log messages can be sent so that some action can be performed on them.

Possible values: ENABLED, DISABLED

lsn Log the LSN messages

Possible values: ENABLED, DISABLED

alg Log the ALG messages

Possible values: ENABLED, DISABLED

subscriberLog Log subscriber session event information

Possible values: ENABLED, DISABLED

sslInterception Log SSL Interception event information

Possible values: ENABLED, DISABLED

urlFiltering Log URL filtering event information

Possible values: ENABLED, DISABLED

ContentInspectionLog Log Content Inspection event information

Possible values: ENABLED, DISABLED

unset audit nslogParams

Removes the existing nslog parameter settings. Attributes for which a default value is available revert to their default values. See the set audit nslogParams command for a description of the parameters..Refer to the set audit nslogParams command for meanings of the arguments.

Synopsis

unset audit nslogParams

show audit nslogParams

Displays the current nslog parameter settings.

Synopsis

show audit nslogParams

Arguments

Output

name Name of the nslog param.

serverIP IP address of the nslog server.

serverPort Port on which the nslog server accepts connections.

dateFormat Format of dates in the logs. Supported formats are:

- MMDDYYYY - U.S. style month/date/year format.
- DDMMYYYY - European style date/month/year format.
- YYYYMMDD - ISO style year/month/date format.

logLevel The audit log level.

logFacility Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the Citrix ADC itself, the VPN, or external.

tcp Configure auditing to log TCP messages.

acl Configure auditing to log access control list (ACL) messages.

timeZone Time zone used for date and timestamps in the logs. Supported settings are:

- GMT_TIME - Coordinated Universal Time.
- LOCAL_TIME - Use the server's timezone setting.

userDefinedAuditlog Log user-configurable log messages to nslog. Setting this parameter to NO causes auditing to ignore all user-configured message actions. Setting this parameter to YES causes auditing to log user-configured message actions that meet the other logging criteria.

appflowExport Export log messages to AppFlow collectors. Appflow collectors are entities to which log messages can be sent so that some action can be performed on them.

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

lsn Log the LSN messages

alg Log the ALG messages

subscriberLog Log subscriber session event information

sslInterception Log SSL Interception event information

urlFiltering Log URL filtering event information

ContentInspectionLog Log Content Inspection event information

audit-nslogPolicy

The following operations can be performed on "audit-nslogPolicy":

add| rm| show| set|

add audit nslogPolicy

Adds a policy that defines which messages to log to the specified nslog server.

Synopsis

add audit nslogPolicy <name> <rule> <action>

Arguments

name Name for the policy. Must begin with a letter, number, or the underscore character (_), and must consist only of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the nslog policy is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my nslog policy" or 'my nslog policy').

rule Name of the Citrix ADC named rule, or an expression, that defines the messages to be logged to the nslog server.

action Nslog server action that is performed when this policy matches. NOTE: An nslog server action must be associated with an nslog audit policy.

rm audit nslogPolicy

Removes the specified nslog policy and associated configuration.

Synopsis

rm audit nslogPolicy <name>

Arguments

name Name of the nslog policy to remove.

show audit nslogPolicy

Displays the current configuration of the specified nslog policy. If no nslog policy is specified, displays a list of all nslog policies currently configured on the Citrix ADC.

Synopsis

show audit nslogPolicy

Arguments

name Name of the policy.

Output

stateflag rule Name of the Citrix ADC named rule, or an expression, that defines the messages to be logged to the nslog server.

action Nslog server action that is performed when this policy matches. NOTE: An nslog server action must be associated with an nslog audit policy.

boundTo The entity name to which policy is bound

activePolicy priority bindPolicyType policyType builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

expressionType Type of policy (Classic/Advanced)

devno count

set audit nslogPolicy

Modifies the specified parametrers of an existing nslog policy.

Synopsis

set audit nslogPolicy <name>

Arguments

name Name of the nslog policy to modify.

rule Name of the Citrix ADC named rule, or an expression, that defines the messages to be logged to the nslog server.

action Nslog server action that is performed when this policy matches. NOTE: An nslog server action must be associated with an nslog audit policy.

audit-stats

The following operations can be performed on "audit-stats":

show audit stats

show audit stats is an alias for stat audit

Synopsis

show audit stats - alias for 'stat audit'

audit-syslogAction

The following operations can be performed on "audit-syslogAction":

show| rm| set| unset| add|

show audit syslogAction

Displays the current configuration of the specified syslog action. If no syslog action is specified, displays a list of all syslog actions currently configured on the Citrix ADC.

Synopsis

show audit syslogAction

Arguments

name Name of the syslog action.

Output

serverIP IP address of the syslog server.

serverDomainName SYSLOG server name as a FQDN. Mutually exclusive with serverIP/ lbVserverName

IP The resolved IP address of the syslog server

lbVserverName Name of the LB vserver. Mutually exclusive with syslog serverIP/serverName

domainResolveRetry Time, in seconds, for which the Citrix ADC waits before sending another DNS query to resolve the host name of the syslog server if the last query failed.

domainResolveNow Immediately send a DNS query to resolve the server's domain name.

serverPort Port on which the syslog server accepts connections.

logLevel Audit log level, which specifies the types of events to log. Available values function as follows:

- ALL - All events.
- EMERGENCY - Events that indicate an immediate crisis on the server.
- ALERT - Events that might require action.
- CRITICAL - Events that indicate an imminent server crisis.
- ERROR - Events that indicate some type of error.
- WARNING - Events that require action in the near future.
- NOTICE - Events that the administrator should know about.
- INFORMATIONAL - All but low-level events.
- DEBUG - All events, in extreme detail.
- NONE - No events.

dateFormat Format of dates in the logs. Supported formats are:

- MMDDYYYY. -U.S. style month/date/year format.
- DDMMYYYY - European style date/month/year format.
- YYYYMMDD - ISO style year/month/date format.

logFacility Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the Citrix ADC itself, the VPN, or external.

tcp Log TCP messages.

acl Log access control list (ACL) messages.

timeZone Time zone used for date and timestamps in the logs. Supported settings are:

- GMT_TIME. Coordinated Universal time.
- LOCAL_TIME. Use the server's timezone setting.

stateflag userDefinedAuditlog Log user-configurable log messages to syslog. Setting this parameter to NO causes auditing to ignore all user-configured message actions. Setting this parameter to YES causes auditing to log user-configured message actions that meet the other logging criteria.

appflowExport Disable export of log messages to AppFlow collectors.

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

lsn Log lsn info

alg Log alg info

subscriberLog Log subscriber session event information

transport Transport type used to send auditlogs to syslog server. Default type is UDP.

tcpProfileName Name of the TCP profile whose settings are to be applied to the audit server info to tune the TCP connection parameters.

maxLogDataSizeToHold Max size of log data that can be held in NSB chain of server info.

dns Log DNS related syslog messages

netProfile Name of the network profile. The SNIP configured in the network profile will be used as source IP while sending log messages.

sslInterception Log SSL Interception event information

urlFiltering Log URL filtering event information

ContentInspectionLog Log Content Inspection event information

devno count

rm audit syslogAction

Removes the specified syslog action and associated configuration. Note: A syslog action cannot be removed if it is bound to a syslog policy.

Synopsis

rm audit syslogAction <name>

Arguments

name Name of the syslog action to remove.

set audit syslogAction

Modifies the specified parameters of an existing syslog action.

Synopsis

set audit syslogAction <name>

Arguments

name Name of the syslog action to be modified.

serverIP IP address of the syslog server.

serverDomainName SYSLOG server name as a FQDN. Mutually exclusive with serverIP/ lbVserverName

lbVserverName Name of the LB vserver. Mutually exclusive with syslog serverIP/serverName

domainResolveRetry Time, in seconds, for which the Citrix ADC waits before sending another DNS query to resolve the host name of the syslog server if the last query failed. Default value: 5 Minimum value: 5 Maximum value: 20939

domainResolveNow Immediately send a DNS query to resolve the server's domain name.

serverPort Port on which the syslog server accepts connections. Minimum value: 1

logLevel Audit log level, which specifies the types of events to log. Available values function as follows:

- ALL - All events.
- EMERGENCY - Events that indicate an immediate crisis on the server.
- ALERT - Events that might require action.
- CRITICAL - Events that indicate an imminent server crisis.
- ERROR - Events that indicate some type of error.
- WARNING - Events that require action in the near future.
- NOTICE - Events that the administrator should know about.
- INFORMATIONAL - All but low-level events.

- DEBUG - All events, in extreme detail.
- NONE - No events.

dateFormat Format of dates in the logs. Supported formats are:

- MMDDYYYY. -U.S. style month/date/year format.
- DDMMYYYY - European style date/month/year format.
- YYYYMMDD - ISO style year/month/date format.

Possible values: MMDDYYYY, DDMMYYYY, YYYYMMDD

logFacility Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the Citrix ADC itself, the VPN, or external.

Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7

tcp Log TCP messages.

Possible values: NONE, ALL

acl Log access control list (ACL) messages.

Possible values: ENABLED, DISABLED

timeZone Time zone used for date and timestamps in the logs. Supported settings are:

- GMT_TIME. Coordinated Universal time.
- LOCAL_TIME. Use the server's timezone setting.

Possible values: GMT_TIME, LOCAL_TIME

userDefinedAuditlog Log user-configurable log messages to syslog. Setting this parameter to NO causes auditing to ignore all user-configured message actions. Setting this parameter to YES causes auditing to log user-configured message actions that meet the other logging criteria.

Possible values: YES, NO

appflowExport Export log messages to AppFlow collectors. Appflow collectors are entities to which log messages can be sent so that some action can be performed on them.

Possible values: ENABLED, DISABLED

lsn Log lsn info

Possible values: ENABLED, DISABLED

alg Log alg info

Possible values: ENABLED, DISABLED

subscriberLog Log subscriber session event information

Possible values: ENABLED, DISABLED

tcpProfileName Name of the TCP profile whose settings are to be applied to the audit server info to tune the TCP connection parameters.

maxLogDataSizeToHold Max size of log data that can be held in NSB chain of server info. Default value: 500 Minimum value: 50 Maximum value: 25600

dns Log DNS related syslog messages

Possible values: ENABLED, DISABLED

ContentInspectionLog Log Content Inspection event information

Possible values: ENABLED, DISABLED

netProfile Name of the network profile. The SNIP configured in the network profile will be used as source IP while sending log messages.

sslInterception Log SSL Interception event information

Possible values: ENABLED, DISABLED

urlFiltering Log URL filtering event information

Possible values: ENABLED, DISABLED

unset audit syslogAction

Removes the settings of an existing syslog action. Attributes for which a default value is available revert to their default values. See the set audit syslogAction command for a description of the parameters..Refer to the set audit syslogAction command for meanings of the arguments.

Synopsis

unset audit syslogAction <name>

add audit syslogAction

Adds a syslog action. The action contains a reference to a syslog server, and specifies which information to log and how to log that information.

Synopsis

add audit syslogAction <name> (<serverIP> | ((<serverDomainName>) | -lbVserverName <string>)) -logLevel <logLevel> ...

Arguments

name Name of the syslog action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the syslog action is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my syslog action" or 'my syslog action').

serverIP IP address of the syslog server.

serverDomainName SYSLOG server name as a FQDN. Mutually exclusive with serverIP/ lbVserverName

domainResolveRetry Time, in seconds, for which the Citrix ADC waits before sending another DNS query to resolve the host name of the syslog server if the last query failed. Default value: 5 Minimum value: 5 Maximum value: 20939

lbVserverName Name of the LB vserver. Mutually exclusive with syslog serverIP/serverName

serverPort Port on which the syslog server accepts connections. Minimum value: 1

logLevel Audit log level, which specifies the types of events to log. Available values function as follows:

- ALL - All events.
- EMERGENCY - Events that indicate an immediate crisis on the server.
- ALERT - Events that might require action.
- CRITICAL - Events that indicate an imminent server crisis.
- ERROR - Events that indicate some type of error.

- WARNING - Events that require action in the near future.
- NOTICE - Events that the administrator should know about.
- INFORMATIONAL - All but low-level events.
- DEBUG - All events, in extreme detail.
- NONE - No events.

dateFormat Format of dates in the logs. Supported formats are:

- MMDDYYYY. -U.S. style month/date/year format.
- DDMMYYYY - European style date/month/year format.
- YYYYMMDD - ISO style year/month/date format.

Possible values: MMDDYYYY, DDMMYYYY, YYYYMMDD

logFacility Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the Citrix ADC itself, the VPN, or external.

Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7

tcp Log TCP messages.

Possible values: NONE, ALL

acl Log access control list (ACL) messages.

Possible values: ENABLED, DISABLED

timeZone Time zone used for date and timestamps in the logs. Supported settings are:

- GMT_TIME. Coordinated Universal time.
- LOCAL_TIME. Use the server's timezone setting.

Possible values: GMT_TIME, LOCAL_TIME

userDefinedAuditlog Log user-configurable log messages to syslog. Setting this parameter to NO causes auditing to ignore all user-configured message actions. Setting this parameter to YES causes auditing to log user-configured message actions that meet the other logging criteria.

Possible values: YES, NO

appflowExport Export log messages to AppFlow collectors. Appflow collectors are entities to which log messages can be sent so that some action can be performed on them.

Possible values: ENABLED, DISABLED

lsn Log lsn info

Possible values: ENABLED, DISABLED

alg Log alg info

Possible values: ENABLED, DISABLED

subscriberLog Log subscriber session event information

Possible values: ENABLED, DISABLED

transport Transport type used to send auditlogs to syslog server. Default type is UDP.

Possible values: TCP, UDP

tcpProfileName Name of the TCP profile whose settings are to be applied to the audit server info to tune the TCP connection parameters.

maxLogDataSizeToHold Max size of log data that can be held in NSB chain of server info. Default value: 500 Minimum value: 50 Maximum value: 25600

dns Log DNS related syslog messages

Possible values: ENABLED, DISABLED

ContentInspectionLog Log Content Inspection event information

Possible values: ENABLED, DISABLED

netProfile Name of the network profile. The SNIP configured in the network profile will be used as source IP while sending log messages.

sslInterception Log SSL Interception event information

Possible values: ENABLED, DISABLED

urlFiltering Log URL filtering event information

Possible values: ENABLED, DISABLED

audit-syslogGlobal

The following operations can be performed on "audit-syslogGlobal":

show| unbind| bind|

show audit syslogGlobal

Displays the list of policies bound to the specified audit syslogGlobal bind point.

Synopsis

show audit syslogGlobal

Arguments

Output

stateflag policyName Name of the audit syslog policy.

priority Specifies the priority of the policy.

numpol number of polices bound to label.

flags globalBindType type The bindpoint to which the policy is bound

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

devno count

Example

show audit syslogGlobal

unbind audit syslogGlobal

Unbind the specified audit syslog policy from audit syslogGlobal.

Synopsis

unbind audit syslogGlobal

Arguments

policyName Name of the policy to unbind.

globalBindType

Example

unbind audit syslogGlobal pol9

bind audit syslogGlobal

binds audit syslog policy to audit syslogGlobal

Synopsis

bind audit syslogGlobal -policyName <string> -priority <positive_integer>

Arguments

policyName Name of the audit syslog policy.

priority Specifies the priority of the policy. Minimum value: 1 Maximum value: 2147483647

globalBindType

Example

bind audit syslogGlobal -policyname pol9 -priority 9

audit-syslogParams

The following operations can be performed on "audit-syslogParams":

set| unset| show|

set audit syslogParams

Modifies the syslog parameters. Changes the IP, the port, or the logging parameters for logs sent to syslog.

Synopsis

set audit syslogParams

Arguments

serverIP IP address of the syslog server.

serverPort Port on which the syslog server accepts connections. Minimum value: 1

dateFormat Format of dates in the logs. Supported formats are:

- MMDDYYYY - U.S. style month/date/year format.
- DDMMYYYY. European style -date/month/year format.
- YYYYMMDD - ISO style year/month/date format.

Possible values: MMDDYYYY, DDMMYYYY, YYYYMMDD

logLevel Types of information to be logged. Available settings function as follows:

- ALL - All events.
- EMERGENCY - Events that indicate an immediate crisis on the server.
- ALERT - Events that might require action.
- CRITICAL - Events that indicate an imminent server crisis.
- ERROR - Events that indicate some type of error.
- WARNING - Events that require action in the near future.
- NOTICE - Events that the administrator should know about.
- INFORMATIONAL - All but low-level events.
- DEBUG - All events, in extreme detail.
- NONE - No events.

logFacility Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the Citrix ADC itself, the VPN, or external.

Possible values: LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7

tcp Log TCP messages.

Possible values: NONE, ALL

acl Log access control list (ACL) messages.

Possible values: ENABLED, DISABLED

timeZone Time zone used for date and timestamps in the logs. Available settings function as follows:

- GMT_TIME - Coordinated Universal Time.

- LOCAL_TIME Use the server's timezone setting.

Possible values: GMT_TIME, LOCAL_TIME

userDefinedAuditlog Log user-configurable log messages to syslog. Setting this parameter to NO causes audit to ignore all user-configured message actions. Setting this parameter to YES causes audit to log user-configured message actions that meet the other logging criteria.

Possible values: YES, NO

appflowExport Export log messages to AppFlow collectors. Appflow collectors are entities to which log messages can be sent so that some action can be performed on them.

Possible values: ENABLED, DISABLED

lsn Log the LSN messages

Possible values: ENABLED, DISABLED

alg Log the ALG messages

Possible values: ENABLED, DISABLED

subscriberLog Log subscriber session event information

Possible values: ENABLED, DISABLED

dns Log DNS related syslog messages

Possible values: ENABLED, DISABLED

sslInterception Log SSL Interceptionn event information

Possible values: ENABLED, DISABLED

urlFiltering Log URL filtering event information

Possible values: ENABLED, DISABLED

ContentInspectionLog Log Content Inspection event ifnormation

Possible values: ENABLED, DISABLED

unset audit syslogParams

Removes the existing syslog parameter settings. Attributes for which a default value is available revert to their default values. See the set audit syslogParams command for descriptions of the parameters..Refer to the set audit syslogParams command for meanings of the arguments.

Synopsis

unset audit syslogParams

show audit syslogParams

Displays the current syslog parameter settings.

Synopsis

show audit syslogParams

Arguments

Output

name Name.

serverIP IP address of the syslog server.

serverPort Port on which the syslog server accepts connections.

dateFormat Format of dates in the logs. Supported formats are:

- MMDDYYYY - U.S. style month/date/year format.
- DDMMYYYY. European style -date/month/year format.
- YYYYMMDD - ISO style year/month/date format.

logLevel Types of information to be logged. Available settings function as follows:

- ALL - All events.
- EMERGENCY - Events that indicate an immediate crisis on the server.
- ALERT - Events that might require action.
- CRITICAL - Events that indicate an imminent server crisis.
- ERROR - Events that indicate some type of error.
- WARNING - Events that require action in the near future.

- NOTICE - Events that the administrator should know about.
- INFORMATIONAL - All but low-level events.
- DEBUG - All events, in extreme detail.
- NONE - No events.

logFacility Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the Citrix ADC itself, the VPN, or external.

tcp Log TCP messages.

acl Log access control list (ACL) messages.

timeZone Time zone used for date and timestamps in the logs. Available settings function as follows:

- GMT_TIME - Coordinated Universal Time.
- LOCAL_TIME Use the server's timezone setting.

userDefinedAuditlog Log user-configurable log messages to syslog. Setting this parameter to NO causes audit to ignore all user-configured message actions. Setting this parameter to YES causes audit to log user-configured message actions that meet the other logging criteria.

appflowExport Export log messages to AppFlow collectors. Appflow collectors are entities to which log messages can be sent so that some action can be performed on them.

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

lsn Log the LSN messages

alg Log the ALG messages

subscriberLog Log subscriber session event information

dns Log DNS related syslog messages

sslInterception Log SSL Interceptionn event information

urlFiltering Log URL filtering event information

ContentInspectionLog Log Content Inspection event ifnormation

audit-syslogPolicy

The following operations can be performed on "audit-syslogPolicy":

set| rm| show| add|

set audit syslogPolicy

Configures an existing syslog policy.

Synopsis

set audit syslogPolicy <name>

Arguments

name Name of the syslog policy to be configured.

rule Name of the Citrix ADC named rule, or an expression, that defines the messages to be logged to the syslog server.

action Syslog server action to perform when this policy matches traffic. NOTE: A syslog server action must be associated with a syslog audit policy.

rm audit syslogPolicy

Removes the specified syslog policy and associated configuration.

Synopsis

rm audit syslogPolicy <name>

Arguments

name Name of the syslog policy to remove.

show audit syslogPolicy

Displays the current configuration of the specified syslog policy. If no syslog policy is specified, displays a list of all syslog policies currently configured on the Citrix ADC.

Synopsis

show audit syslogPolicy

Arguments

name Name of the policy.

Output

stateflag rule Name of the Citrix ADC named rule, or an expression, that defines the messages to be logged to the syslog server.

action Syslog server action to perform when this policy matches traffic. NOTE: A syslog server action must be associated with a syslog audit policy.

boundTo The entity name to which policy is bound

activePolicy priority bindPolicyType policyType builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

expressionType Type of policy (Classic/Advanced)

devno count

add audit syslogPolicy

Adds a policy that defines which messages to log to the specified syslog server.

Synopsis

add audit syslogPolicy <name> <rule> <action>

Arguments

name Name for the policy. Must begin with a letter, number, or the underscore character (_), and must consist only of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the syslog policy is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my syslog policy" or 'my syslog policy').

rule Name of the Citrix ADC named rule, or an expression, that defines the messages to be logged to the syslog server.

action Syslog server action to perform when this policy matches traffic. NOTE: A syslog server action must be associated with a syslog audit policy.

audit

The following operations can be performed on "audit":

stat audit

Display the audit statistics

Synopsis

stat audit

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Logs sent to syslog server(UDP) (LogSnd) Syslog messages sent to the syslog server(s) over UDP.

Audit log messages generated (LogGen) Syslog messages about to be sent to the syslog server.

Logs sent to syslog server(TCP) (LogSndTcp) Syslog messages sent to the syslog server(s) over TCP.

NAT allocation failed (Ernatpcb) NAT allocation failed.

Nsb allocation failed (Ernsb) Nsb allocation failed.

Memory allocation failed (Ermem) Failures in allocation of Access Gateway context structure. When an Access Gateway session is established, the Citrix ADC creates an internal context structure , which identifies the user and the IP address from which the user has logged in.

Port allocation failed (Erport) Number of times the Citrix ADC failed to allocate a port when sending a syslog message to the syslog server(s).

Context not found (Ctxntfnd) Failures in finding the context structure for an Access Gateway session during attempts to send session-specific audit messages.

During an Access Gateway session, audit messages related to the session are queued up in the auditlog buffer for transmission to the audit log server(s). If the session is killed before the messages are sent, the context structure allocated at session creation is removed. This structure is needed for sending the queued auditlog messages. If it is not found, this counter is incremented.

Nsb chain allocation failed (Ernsbchn) Nsb Chain allocation failed.

Client connect failed (Erclconn) Failures in establishment of a connection between the Citrix ADC and the auditserver tool (the Citrix ADC's custom logging tool).

MP buffer flush command count (flcmdcnt) Auditlog buffer flushes. In a multiprocessor Citrix ADC, both the main processor and the co-processor can generate auditlog messages and fill up the auditlog buffers. But only the primary processor can free up the buffers by sending auditlog messages to the auditlog server(s). The number of auditlog buffers is fixed. If the co-processor detects that all the auditlog buffers are full, it issues a flush command to the main processor.

TCP connect failed for syslog (Ersystcpconn) Failures in establishment of a connection between the Citrix ADC and the syslog server.

Logs unsent to LB syslog server (LogUnsentLBsys) Total auditlog messages which are not delivered to load balanced syslog servers

Logs dropped(max hold limit) (DroppedLogsCnt) Total number of log messages dropped by Citrix ADC after max hold limit is reached

Logs dropped(TX min NSBS) (DroppedLogsCntTxMinNSBs) Total number of log messages dropped by Citrix ADC when NSBQ length is less than TX min NSBs

authentication

authentication-OAuthAction

The following operations can be performed on "authentication-OAuthAction":

unset| rm| add| show| set|

unset authentication OAuthAction

Use this command to remove authentication OAuthAction settings.Refer to the set authentication OAuthAction command for meanings of the arguments.

Synopsis

unset authentication OAuthAction <name>

rm authentication OAuthAction

Removes a OAuth authentication action. You cannot remove an action that is used in any part of a policy.

Synopsis

rm authentication OAuthAction <name>

Arguments

name Name of the OAuth authentication action to remove.

Example

rm authentication OAuthAction a1

add authentication OAuthAction

Adds an action to be used for OAuth authentication.

Synopsis

add authentication OAuthAction <name>

Arguments

name Name for the OAuth Authentication action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the profile is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication action" or 'my authentication action').

OAuthType Type of the OAuth implementation. Default value is generic implementation that is applicable for most deployments.

Possible values: GENERIC, INTUNE, ATHENA Default value: GENERIC

authorizationEndpoint Authorization endpoint/url to which unauthenticated user will be redirected. Citrix ADC redirects user to this endpoint by adding query parameters including clientid. If this parameter not specified then as default value we take Token Endpoint/URL value. Please note that Authorization Endpoint or Token Endpoint is mandatory for oauthAction

tokenEndpoint URL to which OAuth token will be posted to verify its authenticity. User obtains this token from Authorization server upon successful authentication. Citrix ADC will validate presented token by posting it to the URL configured

idtokenDecryptEndpoint URL to which obtained idtoken will be posted to get a decrypted user identity. Encrypted idtoken will be obtained by posting OAuth token to token endpoint. In order to decrypt idtoken, Citrix ADC posts request to the URL configured

clientID Unique identity of the client/user who is getting authenticated. Authorization server infers client configuration using this ID

clientSecret Secret string established by user and authorization server

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

Attribute1 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute1

Attribute2 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute2

Attribute3 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute3

Attribute4 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute4

Attribute5 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute5

Attribute6 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute6

Attribute7 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute7

Attribute8 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute8

Attribute9 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute9

Attribute10 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute10

Attribute11 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute11

Attribute12 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute12

Attribute13 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute13

Attribute14 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute14

Attribute15 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute15

Attribute16 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute16

Attributes List of attribute names separated by ',' which needs to be extracted. Note that preceding and trailing spaces will be removed. Attribute name can be 127 bytes and total length of this string should not cross 1023 bytes. These attributes have multi-value support separated by ',' and stored as key-value pair in AAA session

tenantID TenantID of the application. This is usually specific to providers such as Microsoft and usually refers to the deployment identifier.

GraphEndpoint URL of the Graph API service to learn Enterprise Mobility Services (EMS) endpoints.

refreshInterval Interval at which services are monitored for necessary configuration. Default value: 1440 Minimum value: 0

CertEndpoint URL of the endpoint that contains JWKs (Json Web Key) for JWT (Json Web Token) verification.

audience Audience for which token sent by Authorization server is applicable. This is typically entity name or url that represents the recipient

userNameField Attribute in the token from which username should be extracted.

skewTime This option specifies the allowed clock skew in number of minutes that Citrix ADC allows on an incoming token. For example, if skewTime is 10, then token would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all. Default value: 5

issuer Identity of the server whose tokens are to be accepted.

UserInfoURL URL to which OAuth access token will be posted to obtain user information.

CertFilePath Path to the file that contains JWKs (Json Web Key) for JWT (Json Web Token) verification.

grantType Grant type support. value can be code or password

Possible values: CODE, PASSWORD Default value: CODE

authentication If authentication is disabled, password is not sent in the request.

Possible values: ENABLED, DISABLED Default value: ENABLED

introspectURL URL to which access token would be posted for validation

allowedAlgorithms Multivalued option to specify allowed token verification algorithms. Default value: OAUTH_ALG_ALL

PKCE Option to enable/disable PKCE flow during authentication.

Possible values: ENABLED, DISABLED Default value: ENABLED

tokenEndpointAuthMethod Option to select the variant of token authentication method. This method is used while exchanging code with IdP.

Possible values: client_secret_post, client_secret_jwt, private_key_jwt, client_secret_basic Default value: client_secret_post,

metadataUrl Well-known configuration endpoint of the Authorization Server. Citrix ADC fetches server details from this endpoint.

resourceUri Resource URL for Oauth configuration.

Example

add authentication oauthAction a -authorizationEndpoint https://google.com/ -tokenEndpoint https://google.com/ -clientiD sadf -clientsecret df

show authentication OAuthAction

Displays information about the configured OAuth authentication action.

Synopsis

show authentication OAuthAction

Arguments

name Name of the OAuth authentication action to display. If a name is not provided, information about all actions is shown.

Output

stateflag authorizationEndpoint Authorization endpoint/url to which unauthenticated user will be redirected. Citrix ADC redirects user to this endpoint by adding query parameters including clientid. If this parameter not specified then as default value we take Token Endpoint/URL value. Please note that Authorization Endpoint or Token Endpoint is mandatory for oauthAction

tokenEndpoint URL to which OAuth token will be posted to verify its authenticity. User obtains this token from Authorization server upon successful authentication. Citrix ADC will validate presented token by posting it to the URL configured

idtokenDecryptEndpoint URL to which obtained idtoken will be posted to get a decrypted user identity. Encrypted idtoken will be obtained by posting OAuth token to token endpoint. In order to decrypt idtoken, Citrix ADC posts request to the URL configured

clientID Unique identity of the client/user who is getting authenticated. Authorization server infers client configuration using this ID

clientSecret Secret string established by user and authorization server

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

Attribute1 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute1

Attribute2 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute2

Attribute3 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute3

Attribute4 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute4

Attribute5 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute5

Attribute6 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute6

Attribute7 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute7

Attribute8 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute8

Attribute9 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute9

Attribute10 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute10

Attribute11 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute11

Attribute12 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute12

Attribute13 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute13

Attribute14 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute14

Attribute15 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute15

Attribute16 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute16

Attributes List of attribute names separated by ',' which needs to be extracted. Note that preceding and trailing spaces will be removed. Attribute name can be 127 bytes and total length of this string should not cross 1023 bytes. These attributes have multi-value support separated by ',' and stored as key-value pair in AAA session

tenantID TenantID of the application. This is usually specific to providers such as Microsoft and usually refers to the deployment identifier.

GraphEndpoint URL of the Graph API service to learn Enterprise Mobility Services (EMS) endpoints.

refreshInterval Interval at which services are monitored for necessary configuration.

CertEndpoint URL of the endpoint that contains JWKs (Json Web Key) for JWT (Json Web Token) verification.

OAuthType Type of the OAuth implementation. Default value is generic implementation that is applicable for most deployments.

audience Audience for which token sent by Authorization server is applicable. This is typically entity name or url that represents the recipient

userNameField Attribute in the token from which username should be extracted.

skewTime This option specifies the allowed clock skew in number of minutes that Citrix ADC allows on an incoming token. For example, if skewTime is 10, then token would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all.

issuer Identity of the server whose tokens are to be accepted.

OAuthStatus Describes status information of oauth server.

UserInfoURL URL to which OAuth access token will be posted to obtain user information.

CertFilePath Path to the file that contains JWKs (Json Web Key) for JWT (Json Web Token) verification.

grantType Grant type support. value can be code or password

authentication If authentication is disabled, password is not sent in the request.

introspectURL URL to which access token would be posted for validation

allowedAlgorithms Multivalued option to specify allowed token verification algorithms.

PKCE Option to enable/disable PKCE flow during authentication.

tokenEndpointAuthMethod Option to select the variant of token authentication method. This method is used while exchanging code with IdP.

metadataUrl Well-known configuration endpoint of the Authorization Server. Citrix ADC fetches server details from this endpoint.

resourceUri Resource URL for Oauth configuration.

devno count

Example

show authentication OAuthAction a1

set authentication OAuthAction

Modifies the attributes of an existing OAuth authentication action.

Synopsis

set authentication OAuthAction <name>

Arguments

name Name of the action to configure.

OAuthType Type of the OAuth implementation. Default value is generic implementation that is applicable for most deployments.

Possible values: GENERIC, INTUNE, ATHENA Default value: GENERIC

authorizationEndpoint Authorization endpoint/url to which unauthenticated user will be redirected. Citrix ADC redirects user to this endpoint by adding query parameters including clientid. If this parameter not specified then as default value we take Token Endpoint/URL value. Please note that Authorization Endpoint or Token Endpoint is mandatory for oauthAction

tokenEndpoint URL to which OAuth token will be posted to verify its authenticity. User obtains this token from Authorization server upon successful authentication. Citrix ADC will validate presented token by posting it to the URL configured

idtokenDecryptEndpoint URL to which obtained idtoken will be posted to get a decrypted user identity. Encrypted idtoken will be obtained by posting OAuth token to token endpoint. In order to decrypt idtoken, Citrix ADC posts request to the URL configured

clientID Unique identity of the client/user who is getting authenticated. Authorization server infers client configuration using this ID

clientSecret Secret string established by user and authorization server

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

Attribute1 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute1

Attribute2 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute2

Attribute3 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute3

Attribute4 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute4

Attribute5 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute5

Attribute6 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute6

Attribute7 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute7

Attribute8 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute8

Attribute9 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute9

Attribute10 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute10

Attribute11 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute11

Attribute12 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute12

Attribute13 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute13

Attribute14 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute14

Attribute15 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute15

Attribute16 Name of the attribute to be extracted from OAuth Token and to be stored in the attribute16

Attributes List of attribute names separated by ',' which needs to be extracted. Note that preceding and trailing spaces will be removed. Attribute name can be 127 bytes and total length of this string should not cross 1023 bytes. These attributes have multi-value support separated by ',' and stored as key-value pair in AAA session

tenantID TenantID of the application. This is usually specific to providers such as Microsoft and usually refers to the deployment identifier.

GraphEndpoint URL of the Graph API service to learn Enterprise Mobility Services (EMS) endpoints.

refreshInterval Interval at which services are monitored for necessary configuration. Default value: 1440 Minimum value: 0

CertEndpoint URL of the endpoint that contains JWKs (Json Web Key) for JWT (Json Web Token) verification.

audience Audience for which token sent by Authorization server is applicable. This is typically entity name or url that represents the recipient

userNameField Attribute in the token from which username should be extracted.

skewTime This option specifies the allowed clock skew in number of minutes that Citrix ADC allows on an incoming token. For example, if skewTime is 10, then token would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all. Default value: 5

issuer Identity of the server whose tokens are to be accepted.

UserInfoURL URL to which OAuth access token will be posted to obtain user information.

CertFilePath Path to the file that contains JWKs (Json Web Key) for JWT (Json Web Token) verification.

grantType Grant type support. value can be code or password

Possible values: CODE, PASSWORD Default value: CODE

authentication If authentication is disabled, password is not sent in the request.

Possible values: ENABLED, DISABLED Default value: ENABLED

introspectURL URL to which access token would be posted for validation

allowedAlgorithms Multivalued option to specify allowed token verification algorithms. Default value: OAUTH_ALG_ALL

PKCE Option to enable/disable PKCE flow during authentication.

Possible values: ENABLED, DISABLED Default value: ENABLED

tokenEndpointAuthMethod Option to select the variant of token authentication method. This method is used while exchanging code with IdP.

Possible values: client_secret_post, client_secret_jwt, private_key_jwt, client_secret_basic Default value: client_secret_post,

metadataUrl Well-known configuration endpoint of the Authorization Server. Citrix ADC fetches server details from this endpoint.

resourceUri Resource URL for Oauth configuration.

Example

set authentication OAuthAction a1 -ClientID someid123 -clientSecret somesecret

authentication-OAuthIDPProfile

The following operations can be performed on "authentication-OAuthIDPProfile":

set| rm| add| unset| show|

set authentication OAuthIDPProfile

Modifies the specified attributes of a OAuth IdP profile.

Synopsis

set authentication OAuthIDPProfile <name>

Arguments

name Name for the new OAuth Identity Provider (IdP) single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

clientID Unique identity of the relying party requesting for authentication.

clientSecret Unique secret string to authorize relying party at authorization server.

redirectURL URL endpoint on relying party to which the OAuth token is to be sent.

issuer The name to be used in requests sent fromCitrix ADC to IdP to uniquely identify Citrix ADC.

configservice Name of the entity that is used to obtain configuration for the current authentication request. It is used only in Citrix Cloud.

audience Audience for which token is being sent by Citrix ADC IdP. This is typically entity name or url that represents the recipient

skewTime This option specifies the duration for which the token sent by Citrix ADC IdP is valid. For example, if skewTime is 10, then token would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all. Default value: 5

defaultAuthenticationGroup This group will be part of AAA session's internal group list. This will be helpful to admin in Nfactor flow to decide right AAA configuration for Relaying Party. In authentication policy AAA.USER.IS_MEMBER_OF("<default_auth_group>") is way to use this feature.

relyingPartyMetadataURL This is the endpoint at which Citrix ADC IdP can get details about Relying Party (RP) being configured. Metadata response should include endpoints for jwks_uri for RP public key(s).

refreshInterval Interval at which Relying Party metadata is refreshed. Default value: 50 Minimum value: 0

encryptToken Option to encrypt token when Citrix ADC IDP sends one.

Possible values: ON, OFF Default value: OFF

signatureService Name of the service in cloud used to sign the data. This is applicable only if signature if offloaded to cloud.

signatureAlg Algorithm to be used to sign OpenID tokens.

Possible values: RS256, RS512 Default value: RS256

Attributes Name-Value pairs of attributes to be inserted in idtoken. Configuration format is name=value_expr@@@name2=value2_expr@@@. '@@@' is used as delimiter between Name-Value pairs. name is a literal string whose value is 127 characters and does not contain '=' character. Value is advanced policy expression terminated by @@@ delimiter. Last value need not contain the delimiter.

sendPassword Option to send encrypted password in idtoken.

Possible values: ON, OFF Default value: OFF

rm authentication OAuthIDPProfile

Deletes an existing OAuth IdP profile.

Synopsis

rm authentication OAuthIDPProfile <name>

Arguments

name Name for the new OAuth Identity Provider (IdP) single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

add authentication OAuthIDPProfile

Creates a OAuth IdP profile. This profile is used in verifying incoming authentication request from Reousece Server, and sending token.

Synopsis

add authentication OAuthIDPProfile <name>

Arguments

name Name for the new OAuth Identity Provider (IdP) single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

clientID Unique identity of the relying party requesting for authentication.

clientSecret Unique secret string to authorize relying party at authorization server.

redirectURL URL endpoint on relying party to which the OAuth token is to be sent.

issuer The name to be used in requests sent fromCitrix ADC to IdP to uniquely identify Citrix ADC.

configservice Name of the entity that is used to obtain configuration for the current authentication request. It is used only in Citrix Cloud.

audience Audience for which token is being sent by Citrix ADC IdP. This is typically entity name or url that represents the recipient

skewTime This option specifies the duration for which the token sent by Citrix ADC IdP is valid. For example, if skewTime is 10, then token would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all. Default value: 5

defaultAuthenticationGroup This group will be part of AAA session's internal group list. This will be helpful to admin in Nfactor flow to decide right AAA configuration for Relaying Party. In authentication policy AAA.USER.IS_MEMBER_OF("<default_auth_group>") is way to use this feature.

relyingPartyMetadataURL This is the endpoint at which Citrix ADC IdP can get details about Relying Party (RP) being configured. Metadata response should include endpoints for jwks_uri for RP public key(s).

refreshInterval Interval at which Relying Party metadata is refreshed. Default value: 50 Minimum value: 0

encryptToken Option to encrypt token when Citrix ADC IDP sends one.

Possible values: ON, OFF Default value: OFF

signatureService Name of the service in cloud used to sign the data. This is applicable only if signature if offloaded to cloud.

signatureAlg Algorithm to be used to sign OpenID tokens.

Possible values: RS256, RS512 Default value: RS256

Attributes Name-Value pairs of attributes to be inserted in idtoken. Configuration format is name=value_expr@@@name2=value2_expr@@@. '@@@' is used as delimiter between Name-Value pairs. name is a literal string whose value is 127 characters and does not contain '=' character. Value is advanced policy expression terminated by @@@ delimiter. Last value need not contain the delimiter.

sendPassword Option to send encrypted password in idtoken.

Possible values: ON, OFF Default value: OFF

unset authentication OAuthIDPProfile

Use this command to remove authentication OAuthIDPProfile settings.Refer to the set authentication OAuthIDPProfile command for meanings of the arguments.

Synopsis

unset authentication OAuthIDPProfile <name>

show authentication OAuthIDPProfile

Displays information about all configured OAuth IdP profiles, or displays detailed information about the specified action.

Synopsis

show authentication OAuthIDPProfile

Arguments

name Name for the new OAuth Identity Provider (IdP) single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

Output

clientID Unique identity of the relying party requesting for authentication.

clientSecret Unique secret string to authorize relying party at authorization server.

redirectURL URL endpoint on relying party to which the OAuth token is to be sent.

issuer The name to be used in requests sent fromCitrix ADC to IdP to uniquely identify Citrix ADC.

configservice Name of the entity that is used to obtain configuration for the current authentication request. It is used only in Citrix Cloud.

audience Audience for which token is being sent by Citrix ADC IdP. This is typically entity name or url that represents the recipient

skewTime This option specifies the duration for which the token sent by Citrix ADC IdP is valid. For example, if skewTime is 10, then token would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all.

defaultAuthenticationGroup This group will be part of AAA session's internal group list. This will be helpful to admin in Nfactor flow to decide right AAA configuration for Relaying Party. In authentication policy AAA.USER.IS_MEMBER_OF("<default_auth_group>") is way to use this feature.

relyingPartyMetadataURL This is the endpoint at which Citrix ADC IdP can get details about Relying Party (RP) being configured. Metadata response should include endpoints for jwks_uri for RP public key(s).

refreshInterval Interval at which Relying Party metadata is refreshed.

encryptToken Option to encrypt token when Citrix ADC IDP sends one.

signatureService Name of the service in cloud used to sign the data. This is applicable only if signature if offloaded to cloud.

signatureAlg Algorithm to be used to sign OpenID tokens.

OAuthStatus Describes status information of oauth idp metadata fetch process.

Attributes Name-Value pairs of attributes to be inserted in idtoken. Configuration format is name=value_expr@@@name2=value2_expr@@@. '@@@' is used as delimiter between Name-Value pairs. name is a literal string whose value is 127 characters and does not contain '=' character. Value is advanced policy expression terminated by @@@ delimiter. Last value need not contain the delimiter.

sendPassword Option to send encrypted password in idtoken.

devno count stateflag

authentication-OAuthIdPPolicy

The following operations can be performed on "authentication-OAuthIdPPolicy":

show| rm| set| unset| stat| add| rename|

show authentication OAuthIdPPolicy

Displays information about all configured OAuth Identity Provider (IdP) authentication policies, or displays detailed information about the specified policy.

Synopsis

show authentication OAuthIdPPolicy

Arguments

name Name of the OAuth IdentityProvider (IdP) policy for which to display detailed information.

Output

rule The rule used by the OAuth Identity Provider (IdP) authentication policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide

action The action to be performed when the rule is matched.

stateflag undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only DROP/RESET actions can be used.

comment Any comments to preserve information about this policy.

logAction Name of messagelog action to use when a request matches this policy.

boundTo The entity name to which policy is bound

activePolicy priority gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

hits Number of hits.

bindPolicyType vserverType devno count

rm authentication OAuthIdPPolicy

Removes an existing OAuth Identity Provider (IdP) policy.

Synopsis

rm authentication OAuthIdPPolicy <name>

Arguments

name Name of the authentication policy to remove.

set authentication OAuthIdPPolicy

Modifies the specified parameters of an existing OAuth IdentityProvider (IdP) policy.

Synopsis

set authentication OAuthIdPPolicy <name>

Arguments

name Name of the OAuth Identity Provider (IdP) authentication policy to modify.

rule Expression that the policy uses to determine whether to respond to the specified request.

action Name of the profile to apply to requests or connections that match this policy.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only DROP/RESET actions can be used.

comment Any comments to preserve information about this policy.

logAction Name of messagelog action to use when a request matches this policy.

unset authentication OAuthIdPPolicy

Removes the settings of an existing OAuth IdentityProvider (IdP) policy. Attributes for which a default value is available revert to their default values. See the set OAuthIdPPolicy command for a description of the parameters..Refer to the set authentication OAuthIdPPolicy command for meanings of the arguments.

Synopsis

unset authentication OAuthIdPPolicy <name>

Example

unset OAuthIdpPolicy pol9 -undefAction

stat authentication OAuthIdPPolicy

Display OAUTH Identity Provider (IdP) policy statistics.

Synopsis

stat authentication OAuthIdPPolicy

Arguments

name The name of the OAuth Identity Provider (IdP) policy for which statistics will be displayed. If not given statistics are shown for all policies.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Policy undef hits (Undefhits) Number of undef hits on the policy

Example

stat authentication oauthidppolicy.

Related Commands

- stat authentication loginSchemaPolicy

add authentication OAuthIdPPolicy

Adds a OAuth Identity Provider (IdP) policy to use for use in authentication.

Synopsis

add authentication OAuthIdPPolicy <name> -rule <expression> -action <string>

Arguments

name Name for the OAuth Identity Provider (IdP) authentication policy. This is used for configuring Citrix ADC as OAuth Identity Provider. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

rule Expression that the policy uses to determine whether to respond to the specified request.

action Name of the profile to apply to requests or connections that match this policy.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only DROP/RESET actions can be used.

comment Any comments to preserve information about this policy.

logAction Name of messagelog action to use when a request matches this policy.

rename authentication OAuthIdPPolicy

Renames the specified OAuth IdentityProvider (IdP) policy. You must restart the Citrix ADC to put new name in effect.

Synopsis

rename authentication OAuthIdPPolicy <name>@ <newName>@

Arguments

name Existing name of the OAuth IdentityProvider policy.

newName New name for the OAuth IdentityProvider policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my oauthidppolicy policy" or 'my oauthidppolicy policy').

Example

rename oauthidppolicy policy oldname newname

authentication-Policy

The following operations can be performed on "authentication-Policy":

rename| stat| rm| unset| add| set| show|

rename authentication Policy

Renames the specified authentication policy.

Synopsis

rename authentication Policy <name>@ <newName>@

Arguments

name Existing name of the authentication policy.

newName New name for the authentication policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

Example

rename authentication policy oldname newname

stat authentication Policy

Displays authentication statistics for all advanced authentication policies, or for only the specified policy.

Synopsis

stat authentication Policy

Arguments

name Name of the advanced authentication policy for which to display statistics. If no name is specified, statistics for all advanced authentication polices are shown.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Policy undef hits (Undefhits) Number of undef hits on the policy

Example

stat authentication policy

Related Commands

- stat authentication OAuthIdPPolicy

rm authentication Policy

Removes the advance authentication policy.

Synopsis

rm authentication Policy <name>

Arguments

name Name of the advance authentication policy to remove.

unset authentication Policy

Use this command to remove authentication Policy settings.Refer to the set authentication Policy command for meanings of the arguments.

Synopsis

unset authentication Policy <name>

add authentication Policy

Adds an advanced authentication policy. The policy defines the criteria under which the Citrix ADC attempts to authenticate the user.

Synopsis

add authentication Policy <name> -rule <expression> -action <string>

Arguments

name Name for the advance AUTHENTICATION policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after AUTHENTICATION policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the AUTHENTICATION server.

action Name of the authentication action to be performed if the policy matches.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

comment Any comments to preserve information about this policy.

logAction Name of messagelog action to use when a request matches this policy.

set authentication Policy

Modifies the specified parameters of a authentication policy.

Synopsis

set authentication Policy <name>

Arguments

name Name of the advance authentication policy to modify.

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the AUTHENTICATION server.

action Name of the authentication action to be performed if the policy matches.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

comment Any comments to preserve information about this policy.

logAction Name of messagelog action to use when a request matches this policy.

show authentication Policy

Displays the current settings for the specified advance authentication policy. If no policy name is provided, displays a list of all advance authentication policies currently configured on the Citrix ADC.

Synopsis

show authentication Policy

Arguments

name Name of the advance authentication policy.

Output

rule The name of the new rule associated with the policy.

action The name of the authentication action associated with the policy.

stateflag undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

comment Any comments to preserve information about this policy.

logAction Name of messagelog action to use when a request matches this policy.

hits Number of hits.

boundTo The entity name to which policy is bound

activePolicy priority bindPolicyType policyType nextFactor On success invoke label.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

description Description of the policy

vserverType policySubType type devno count

authentication-adfsProxyProfile

The following operations can be performed on "authentication-adfsProxyProfile":

set| show| add| rm|

set authentication adfsProxyProfile

Set/modify adfsproxyprofile properties.

Synopsis

set authentication adfsProxyProfile <name>

Arguments

name Name for the adfs proxy profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after the profile is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my push service" or 'my push service').

userName This is the name of an account in directory that would be used to authenticate trust request from ADC acting as a proxy.

password This is the password of an account in directory that would be used to authenticate trust request from ADC acting as a proxy.

serverURL Fully qualified url of the adfs server.

CertKeyName SSL certificate of the proxy that is registered at adfs server for trust.

Example

set authentication adfsproxyprofile <profile name> -serverurl <>

show authentication adfsProxyProfile

Displays all the configured adfsproxyprofile entities in the system. If a name is specified, then only that entity is shown.

Synopsis

show authentication adfsProxyProfile

Arguments

name Name of the adfsproxyprofile.

Output

userName This is the name of an account in directory that would be used to authenticate trust request from ADC acting as a proxy.

password This is the password of an account in directory that would be used to authenticate trust request from ADC acting as a proxy.

serverURL Fully qualified url of the adfs server.

CertKeyName SSL certificate of the proxy that is registered at adfs server for trust.

adfsTrustStatus Describes status of ADFS trust.

stateflag State flag

devno count

Example

show authentication adfsproxyprofile

add authentication adfsProxyProfile

Add a new adfsproxy profile on the Citrix ADC.

Synopsis

add authentication adfsProxyProfile <name> -userName <string> -password -serverURL <string> -CertKeyName <string>

Arguments

name Name for the adfs proxy profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after the profile is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my push service" or 'my push service').

userName This is the name of an account in directory that would be used to authenticate trust request from ADC acting as a proxy.

password This is the password of an account in directory that would be used to authenticate trust request from ADC acting as a proxy.

serverURL Fully qualified url of the adfs server.

CertKeyName SSL certificate of the proxy that is registered at adfs server for trust.

Example

add authentication adfsproxyprofile <name> -username <> -password <> -serverurl <> -certificate <>

rm authentication adfsProxyProfile

Remove previously configured adfsproxy profile on Citrix ADC.

Synopsis

rm authentication adfsProxyProfile <name>

Arguments

name Name of the adfsproxy profile.

Example

rm authentication adfsproxyprofile <name>

authentication-authnProfile

The following operations can be performed on "authentication-authnProfile":

set| rm| show| add| unset|

set authentication authnProfile

Configures an authentication profile.

Synopsis

set authentication authnProfile <name>

Arguments

name Name of the authentication profile.

authnVsName Name of the authentication vserver at which authentication should be done. Maximum value: 128

AuthenticationHost Hostname of the authentication vserver to which user must be redirected for authentication. Maximum value: 256

AuthenticationDomain Domain for which TM cookie must to be set. If unspecified, cookie will be set for FQDN. Maximum value: 256

AuthenticationLevel Authentication weight or level of the vserver to which this will bound. This is used to order TM vservers based on the protection required. A session that is created by authenticating against TM vserver at given level cannot be used to access TM vserver at a higher level. Minimum value: 0 Maximum value: 255

rm authentication authnProfile

Removes an authentication profile. A profile cannot be removed as long as it is set to a vserver.

Synopsis

rm authentication authnProfile <name>

Arguments

name Name of the authentication profile to be removed.

show authentication authnProfile

Displays the current configuration for the authentication profile specified

Synopsis

show authentication authnProfile

Arguments

name Name of the authentication profile.

Output

authnVsName Name of the authentication vserver at which authentication should be done.

AuthenticationHost Hostname of the authentication vserver to which user must be redirected for authentication.

AuthenticationDomain Domain for which TM cookie must to be set. If unspecified, cookie will be set for FQDN.

AuthenticationLevel Authentication weight or level of the vserver to which this will bound. This is used to order TM vservers based on the protection required. A session that is created by authenticating against TM vserver at given level cannot be used to access TM vserver at a higher level.

devno count stateflag

add authentication authnProfile

Creates an authentication profile to hold all authentication related configuration for TM vserver.

Synopsis

add authentication authnProfile <name> {-authnVsName <string>} {-AuthenticationHost <string>} {-AuthenticationDomain <string>}

Arguments

name Name for the authentication profile. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the RADIUS action is added.

authnVsName Name of the authentication vserver at which authentication should be done. Maximum value: 128

AuthenticationHost Hostname of the authentication vserver to which user must be redirected for authentication. Maximum value: 256

AuthenticationDomain Domain for which TM cookie must to be set. If unspecified, cookie will be set for FQDN. Maximum value: 256

AuthenticationLevel Authentication weight or level of the vserver to which this will bound. This is used to order TM vservers based on the protection required. A session that is created by authenticating against TM vserver at given level cannot be used to access TM vserver at a higher level. Minimum value: 0 Maximum value: 255

unset authentication authnProfile

Use this command to remove authentication authnProfile settings.Refer to the set authentication authnProfile command for meanings of the arguments.

Synopsis

unset authentication authnProfile <name>

authentication-azureKeyVault

The following operations can be performed on "authentication-azureKeyVault":

rm| set| show| add| unset|

rm authentication azureKeyVault

Deletes an existing Azure key vault.

Synopsis

rm authentication azureKeyVault <name>

Arguments

name Name for the new Azure Key Vault profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

set authentication azureKeyVault

Modifies the specified attributes of an Azure key vault.

Synopsis

set authentication azureKeyVault <name>

Arguments

name Name for the new Azure Key Vault profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

vaultName Name of the Azure vault account as configured in azure portal.

clientID Unique identity of the relying party requesting for authentication.

clientSecret Unique secret string to authorize relying party at authorization server.

serviceKeyName Friendly name of the Key to be used to compute signature.

signatureAlg Algorithm to be used to sign/verify transactions

Possible values: RS256 Default value: RS256

tokenEndpoint URL endpoint on relying party to which the OAuth token is to be sent.

pushService Name of the service used to send push notifications

defaultAuthenticationGroup This is the group that is added to user sessions that match current IdP policy. It can be used in policies to identify relying party trust.

refreshInterval Interval at which access token in obtained. Default value: 50 Minimum value: 0

tenantID TenantID of the application. This is usually specific to providers such as Microsoft and usually refers to the deployment identifier.

authentication If authentication is disabled, otp checks are not performed after azure vault keys are obtained. This is useful to distinguish whether user has registered devices.

Possible values: ENABLED, DISABLED Default value: ENABLED

show authentication azureKeyVault

Displays information about all configured Azure key vaults, or displays detailed information about the specified vault.

Synopsis

show authentication azureKeyVault

Arguments

name Name for the new Azure Key Vault profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

Output

vaultName Name of the Azure vault account as configured in azure portal.

clientID Unique identity of the relying party requesting for authentication.

clientSecret Unique secret string to authorize relying party at authorization server.

serviceKeyName Friendly name of the Key to be used to compute signature.

signatureAlg Algorithm to be used to sign/verify transactions

tokenEndpoint URL endpoint on relying party to which the OAuth token is to be sent.

pushService Name of the service used to send push notifications

defaultAuthenticationGroup This is the group that is added to user sessions that match current IdP policy. It can be used in policies to identify relying party trust.

refreshInterval Interval at which access token in obtained.

tenantID TenantID of the application. This is usually specific to providers such as Microsoft and usually refers to the deployment identifier.

authentication If authentication is disabled, otp checks are not performed after azure vault keys are obtained. This is useful to distinguish whether user has registered devices.

devno count stateflag

add authentication azureKeyVault

Creates a Azure key vault profile. This profile is used to interact with azure services for data signature and storage.

Synopsis

add authentication azureKeyVault <name> -vaultName <string> -clientID <string> -clientSecret -serviceKeyName <string>

Arguments

name Name for the new Azure Key Vault profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

vaultName Name of the Azure vault account as configured in azure portal.

clientID Unique identity of the relying party requesting for authentication.

clientSecret Unique secret string to authorize relying party at authorization server.

serviceKeyName Friendly name of the Key to be used to compute signature.

signatureAlg Algorithm to be used to sign/verify transactions

Possible values: RS256 Default value: RS256

tokenEndpoint URL endpoint on relying party to which the OAuth token is to be sent.

pushService Name of the service used to send push notifications

defaultAuthenticationGroup This is the group that is added to user sessions that match current IdP policy. It can be used in policies to identify relying party trust.

refreshInterval Interval at which access token in obtained. Default value: 50 Minimum value: 0

tenantID TenantID of the application. This is usually specific to providers such as Microsoft and usually refers to the deployment identifier.

authentication If authentication is disabled, otp checks are not performed after azure vault keys are obtained. This is useful to distinguish whether user has registered devices.

Possible values: ENABLED, DISABLED Default value: ENABLED

unset authentication azureKeyVault

Use this command to remove authentication azureKeyVault settings.Refer to the set authentication azureKeyVault command for meanings of the arguments.

Synopsis

unset authentication azureKeyVault <name>

authentication-captchaAction

The following operations can be performed on "authentication-captchaAction":

rm| add| show| unset| set|

rm authentication captchaAction

Deletes an existing captcha action.

Synopsis

rm authentication captchaAction <name>

Arguments

name Name for the new captcha action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space,

colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

add authentication captchaAction

Creates a captcha action.

Synopsis

add authentication captchaAction <name> -secretKey -siteKey

Arguments

name Name for the new captcha action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

serverURL This is the endpoint at which captcha response is validated.

secretKey Secret of gateway as established at the captcha source.

siteKey Sitekey to identify gateway fqdn while loading captcha.

defaultAuthenticationGroup This is the group that is added to user sessions that match current policy.

show authentication captchaAction

Displays information about all configured actions, or displays detailed information about the specified action.

Synopsis

show authentication captchaAction

Arguments

name Name for the new captcha action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

Output

serverURL This is the endpoint at which captcha response is validated.

secretKey Secret of gateway as established at the captcha source.

siteKey Sitekey to identify gateway fqdn while loading captcha.

defaultAuthenticationGroup This is the group that is added to user sessions that match current policy.

devno count stateflag

unset authentication captchaAction

Use this command to remove authentication captchaAction settings.Refer to the set authentication captchaAction command for meanings of the arguments.

Synopsis

unset authentication captchaAction <name>

set authentication captchaAction

Modifies the specified attributes of a captcha action.

Synopsis

set authentication captchaAction <name>

Arguments

name Name for the new captcha action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space,

colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

serverURL This is the endpoint at which captcha response is validated.

secretKey Secret of gateway as established at the captcha source.

siteKey Sitekey to identify gateway fqdn while loading captcha.

defaultAuthenticationGroup This is the group that is added to user sessions that match current policy.

authentication-certAction

The following operations can be performed on "authentication-certAction":

rm| set| add| show| unset|

rm authentication certAction

Removes an existing client cert authentication server profile (action).

Synopsis

rm authentication certAction <name>

Arguments

name Name of the profile to be removed.

set authentication certAction

Configures a client cert authentication server profile (action).

Synopsis

set authentication certAction <name>

Arguments

name Name of the client cert server profile.

twoFactor Enables or disables two-factor authentication. Two factor authentication is client cert authentication followed by password authentication.

Possible values: ON, OFF Default value: OFF

userNameField Client-cert field from which the username is extracted. Must be set to either ""Subject"" and ""Issuer"" (include both sets of double quotation marks). Format: <field>:<subfield>.

groupNameField Client-cert field from which the group is extracted. Must be set to either ""Subject"" and ""Issuer"" (include both sets of double quotation marks). Format: <field>:<subfield>

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

Example

set authentication certaction -twoFactor ON -userNameField "Subject:CN" -groupNameField "Subject:OU"

Related Commands

- add authentication certpolicy

add authentication certAction

Adds an action (profile) for a client certificate (cert) authentication server. The profile contains all configuration data necessary to communicate with that client cert authentication server.

Synopsis

add authentication certAction <name>

Arguments

name Name for the client cert authentication server profile (action). Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after certifcate action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication action" or 'my authentication action').

twoFactor Enables or disables two-factor authentication. Two factor authentication is client cert authentication followed by password authentication.

Possible values: ON, OFF Default value: OFF

userNameField Client-cert field from which the username is extracted. Must be set to either ""Subject"" and ""Issuer"" (include both sets of double quotation marks). Format: <field>:<subfield>.

groupNameField Client-cert field from which the group is extracted. Must be set to either ""Subject"" and ""Issuer"" (include both sets of double quotation marks). Format: <field>:<subfield>

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

Example

add authentication certaction -twoFactor ON -userNameField "Subject:CN" -groupNameField "Subject:OU"

Related Commands

- add authentication certpolicy

show authentication certAction

Displays the current configuration settings for the specified client cert authentication server profile (action).

Synopsis

show authentication certAction

Arguments

name Name of the client cert server profile (action).

Output

twoFactor The state of two factor authentication.

userNameField The field in the certificate from which the username will be extracted.

groupNameField The field in the certificate from which the group will be extracted.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

stateflag devno count

unset authentication certAction

Use this command to remove authentication certAction settings.Refer to the set authentication certAction command for meanings of the arguments.

Synopsis

unset authentication certAction <name>

authentication-certPolicy

The following operations can be performed on "authentication-certPolicy":

set| show| add| unset| rm|

set authentication certPolicy

Configures the specified client cert authentication policy.

Synopsis

set authentication certPolicy <name>

Arguments

name Name of the client cert policy.

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the authentication server.

reqAction Name of the client cert authentication action to be performed if the policy matches.

show authentication certPolicy

Displays the current settings for the specified client cert authentication policy. If no policy name is provided, displays a list of all client cert authentication policies currently configured on the Citrix ADC.

Synopsis

show authentication certPolicy

Arguments

name Name of the client cert authentication policy.

Output

rule The rule associated with the policy.

reqAction The cert action associated with the policy.

boundTo The entity name to which policy is bound

activePolicy priority bindPolicyType policyType devno count stateflag

add authentication certPolicy

Adds a client certificate (cert) authentication policy. The policy defines the criteria under which the Citrix ADC attempts to authenticate the user with the specified client cert authentication server.

Synopsis

add authentication certPolicy <name> <rule>

Arguments

name Name for the client certificate authentication policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after cert authentication policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the authentication server.

reqAction Name of the client cert authentication action to be performed if the policy matches.

unset authentication certPolicy

Use this command to remove authentication certPolicy settings.Refer to the set authentication certPolicy command for meanings of the arguments.

Synopsis

unset authentication certPolicy <name>

rm authentication certPolicy

Removes a client cert authentication policy.

Synopsis

rm authentication certPolicy <name>

Arguments

name Name of the client cert policy to remove.

authentication-citrixAuthAction

The following operations can be performed on "authentication-citrixAuthAction":

add| unset| rm| show| set|

add authentication citrixAuthAction

Creates a Citrix Authentication action. This profile is used to interact with Citrix services for validating user credentials.

Synopsis

add authentication citrixAuthAction <name>

Arguments

name Name for the new Citrix Authentication action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

authenticationType Type of the Citrix Authentication implementation. Default implementation uses Citrix Cloud Connector.

Possible values: CITRIXCONNECTOR, ATHENA Default value: CITRIXCONNECTOR

authentication Authentication needs to be disabled for searching user object without performing authentication.

Possible values: ENABLED, DISABLED Default value: ENABLED

unset authentication citrixAuthAction

Use this command to remove authentication citrixAuthAction settings.Refer to the set authentication citrixAuthAction command for meanings of the arguments.

Synopsis

unset authentication citrixAuthAction <name>

rm authentication citrixAuthAction

Deletes an existing Citrix authentication action.

Synopsis

rm authentication citrixAuthAction <name>

Arguments

name Name for the new Citrix Authentication action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

show authentication citrixAuthAction

Displays information about all configured Citrix authentication actions, or displays detailed information about specified action.

Synopsis

show authentication citrixAuthAction

Arguments

name Name for the new Citrix Authentication action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

Output

authenticationType Type of the Citrix Authentication implementation. Default implementation uses Citrix Cloud Connector.

authentication Authentication needs to be disabled for searching user object without performing authentication.

devno count stateflag

set authentication citrixAuthAction

Modifies the specified attributes of an Azure key vault.

Synopsis

set authentication citrixAuthAction <name>

Arguments

name Name for the new Citrix Authentication action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

authenticationType Type of the Citrix Authentication implementation. Default implementation uses Citrix Cloud Connector.

Possible values: CITRIXCONNECTOR, ATHENA Default value: CITRIXCONNECTOR

authentication Authentication needs to be disabled for searching user object without performing authentication.

Possible values: ENABLED, DISABLED Default value: ENABLED

Authentication

The entities on which you can perform NetScaler CLI operations:

- authentication-OAuthAction
- authentication-OAuthIDPProfile
- authentication-OAuthIdPPolicy
- authentication-Policy
- authentication-adfsProxyProfile
- authentication-authnProfile
- authentication-azureKeyVault
- authentication-captchaAction
- authentication-certAction
- authentication-certPolicy
- authentication-citrixAuthAction
- authentication-dfaAction
- authentication-dfaPolicy
- authentication-emailAction
- authentication-epaAction
- authentication-ldapAction
- authentication-ldapPolicy
- authentication-localPolicy
- authentication-loginSchema
- authentication-loginSchemaPolicy
- authentication-negotiateAction
- authentication-negotiatePolicy
- authentication-noAuthAction
- authentication-policylabel

- authentication-pushService
- authentication-radiusAction
- authentication-radiusPolicy
- authentication-samlAction
- authentication-samlIdPPolicy
- authentication-samlIdPProfile
- authentication-samlPolicy
- authentication-smartAccessPolicy
- authentication-smartAccessProfile
- authentication-storefrontAuthAction
- authentication-tacacsAction
- authentication-tacacsPolicy
- authentication-vserver
- authentication-webAuthAction
- authentication-webAuthPolicy

authentication-dfaAction

The following operations can be performed on "authentication-dfaAction":

rm| show| add| set| unset|

rm authentication dfaAction

Removes a DFA profile (action). An action cannot be removed as long as it is bound to a policy.

Synopsis

rm authentication dfaAction <name>

Arguments

name Name of the action to be removed.

show authentication dfaAction

Displays the current configuration settings for the specified DFA profile (action).

Synopsis

show authentication dfaAction

Arguments

name Name of the DFA profile.

Output

passPhrase Key shared between the DFA server and the Citrix ADC. Required to allow the Citrix ADC to communicate with the DFA server.

clientID If configured, this string is sent to the DFA server as the X-Citrix-Exchange header value.

serverURL DFA Server URL

Success Failure stateflag defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

devno count

add authentication dfaAction

Creates an action (profile) for a DFA server. The profile contains all configuration data necessary to communicate with that DFA server.

Synopsis

add authentication dfaAction <name> {-clientID <string>} {-serverURL <URL>} {-passPhrase }

Arguments

name Name for the DFA action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the DFA action is added.

clientID If configured, this string is sent to the DFA server as the X-Citrix-Exchange header value.

serverURL DFA Server URL

passPhrase Key shared between the DFA server and the Citrix ADC. Required to allow the Citrix ADC to communicate with the DFA server.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

set authentication dfaAction

Configures a DFA server profile (action). The profile contains all configuration data needed to communicate with that DFA server.

Synopsis

set authentication dfaAction <name> {-passPhrase }

Arguments

name Name of the RADIUS profile.

clientID If configured, this string is sent to the DFA server as the X-Citrix-Exchange header value.

serverURL DFA Server URL

passPhrase Key shared between the DFA server and the Citrix ADC. Required to allow the Citrix ADC to communicate with the DFA server.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

unset authentication dfaAction

Use this command to remove authentication dfaAction settings.Refer to the set authentication dfaAction command for meanings of the arguments.

Synopsis

unset authentication dfaAction <name>

authentication-dfaPolicy

The following operations can be performed on "authentication-dfaPolicy":

add| set| rm| show|

add authentication dfaPolicy

Adds an DFA authentication policy. The policy defines the criteria under which the Citrix ADC attempts to authenticate the user with the specified Web server.

Synopsis

add authentication dfaPolicy <name> -rule <string> -action <string>

Arguments

name Name for the DFA policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after DFA policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the Web server.

action Name of the DFA action to perform if the policy matches.

set authentication dfaPolicy

Configures the specified DFA policy.

Synopsis

set authentication dfaPolicy <name>

Arguments

name Name of the DFA policy.

rule The new rule to associate with the policy.

action The new DFA action to associate with the policy.

rm authentication dfaPolicy

Removes an DFA policy.

Synopsis

rm authentication dfaPolicy <name>

Arguments

name Name of the DFA policy to remove.

show authentication dfaPolicy

Displays the current settings for the specified DFA policy. If no policy name is provided, displays a list of all DFA policies currently configured on the Citrix ADC.

Synopsis

show authentication dfaPolicy

Arguments

name Name of the WebAuth policy.

Output

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the Web server.

action Name of the DFA action to perform if the policy matches.

boundTo The entity name to which policy is bound

activePolicy priority bindPolicyType policyType devno count stateflag

authentication-emailAction

The following operations can be performed on "authentication-emailAction":

add| show| unset| set| rm|

add authentication emailAction

Adds an email action that is used to send email to end users.

Synopsis

add authentication emailAction <name> -userName <string> -password -serverURL <string>

Arguments

name Name for the new email action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

userName Username/Clientid/EmailID to be used to authenticate to the server.

password Password/Clientsecret to use when authenticating to the server.

serverURL Address of the server that delivers the message. It is fully qualified fqdn such as http(s):// or smtp(s):// for http and smtp protocols respectively. For SMTP, the port number is mandatory like smtps://smtp.example.com:25.

content Content to be delivered to the user. "$code" string within the content will be replaced with the actual one-time-code to be sent.

defaultAuthenticationGroup This is the group that is added to user sessions that match current IdP policy. It can be used in policies to identify relying party trust.

type Type of the email action. Default type is SMTP.

Possible values: SMTP, ATHENA Default value: SMTP

emailAddress An optional expression that yields user's email. When not configured, user's default mail address would be used. When configured, result of this expression is used as destination email address.

Example

To send email containing OTP for authentication purpose using Secure SMTP server smtp.example.com with port 25, and sender email id is sender@example.com with expression: add authentication emailAction emailact -userName sender@example.com -password <Password> -serverURL "smtps://smtp.example.com:25" -content "OTP is $code" -emailAddress aaa.user.attribute("alternate_mail")

To send email containing OTP for authentication purpose using Secure SMTP server smtp.example.com with port 25, and sender email id is sender@example.com without expression (send to Default mail id): add authentication emailAction emailact -userName sender@example.com -password <Password> -serverURL "smtps://smtp.example.com:25" -content "OTP is $code"

show authentication emailAction

Displays information about all configured email actions, or displays detailed information about the specified action.

Synopsis

show authentication emailAction

Arguments

name Name for the new email action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

Output

userName Username/Clientid/EmailID to be used to authenticate to the server.

password Password/Clientsecret to use when authenticating to the server.

serverURL Address of the server that delivers the message. It is fully qualified fqdn such as http(s):// or smtp(s):// for http and smtp protocols respectively. For SMTP, the port number is mandatory like smtps://smtp.example.com:25.

content Content to be delivered to the user. "$code" string within the content will be replaced with the actual one-time-code to be sent.

defaultAuthenticationGroup This is the group that is added to user sessions that match current IdP policy. It can be used in policies to identify relying party trust.

timeout Time after which the code expires.

type Type of the email action. Default type is SMTP.

emailAddress An optional expression that yields user's email. When not configured, user's default mail address would be used. When configured, result of this expression is used as destination email address.

devno count stateflag

Example

show authentication emailAction emailact

unset authentication emailAction

Use this command to remove authentication emailAction settings.Refer to the set authentication emailAction command for meanings of the arguments.

Synopsis

unset authentication emailAction <name>

set authentication emailAction

Modifies the specified attributes of an email action.

Synopsis

set authentication emailAction <name>

Arguments

name Name for the new email action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

userName Username/Clientid/EmailID to be used to authenticate to the server.

password Password/Clientsecret to use when authenticating to the server.

serverURL Address of the server that delivers the message. It is fully qualified fqdn such as http(s):// or smtp(s):// for http and smtp protocols respectively. For SMTP, the port number is mandatory like smtps://smtp.example.com:25.

content Content to be delivered to the user. "$code" string within the content will be replaced with the actual one-time-code to be sent.

defaultAuthenticationGroup This is the group that is added to user sessions that match current IdP policy. It can be used in policies to identify relying party trust.

type Type of the email action. Default type is SMTP.

Possible values: SMTP, ATHENA Default value: SMTP

emailAddress An optional expression that yields user's email. When not configured, user's default mail address would be used. When configured, result of this expression is used as destination email address.

Example

set authentication emailAction emailact -userName sender@example.com -password <Password> -serverURL "smtps://smtp.example.com:25" -content "OTP is $code" -emailAddress aaa.user.attribute("attrib2")

rm authentication emailAction

Deletes an existing email action.

Synopsis

rm authentication emailAction <name>

Arguments

name Name for the new email action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

Example

rm authentication emailAction emailact

authentication-epaAction

The following operations can be performed on "authentication-epaAction":

show| set| unset| rm| add|

show authentication epaAction

Displays details of the specified epa action.

Synopsis

show authentication epaAction

Arguments

name Name of the epa action.

Output

killProcess String specifying the name of a process to be terminated by the endpoint analysis (EPA) tool. Multiple processes to be delimited by comma

deletefiles String specifying the path(s) and name(s) of the files to be deleted by the endpoint analysis (EPA) tool. Multiple files to be delimited by comma

stateflag defaultEPAGroup This is the default group that is chosen when the EPA check succeeds.

quarantineGroup This is the quarantine group that is chosen when the EPA check fails if configured.

csecexpr it holds the ClientSecurityExpression to be sent to the client

devno count

set authentication epaAction

Modifies an existing epa action (profile).

Synopsis

set authentication epaAction <name>

Arguments

name Name of the epa action to modify.

csecexpr it holds the ClientSecurityExpression to be sent to the client

killProcess String specifying the name of a process to be terminated by the endpoint analysis (EPA) tool. Multiple processes to be delimited by comma

deletefiles String specifying the path(s) and name(s) of the files to be deleted by the endpoint analysis (EPA) tool. Multiple files to be delimited by comma

defaultEPAGroup This is the default group that is chosen when the EPA check succeeds. Maximum value: 64

quarantineGroup This is the quarantine group that is chosen when the EPA check fails if configured. Maximum value: 64

unset authentication epaAction

Use this command to remove authentication epaAction settings.Refer to the set authentication epaAction command for meanings of the arguments.

Synopsis

unset authentication epaAction <name>

rm authentication epaAction

Removes an epa action. NOTE: An epa action cannot be removed if it is bound to a policy.

Synopsis

rm authentication epaAction <name>

Arguments

name Name of the epa action to remove.

add authentication epaAction

Adds an action (profile) for endpoint analysis (EPA) clients before authentication.

Synopsis

add authentication epaAction <name> -csecexpr <expression>

Arguments

name Name for the epa action. Must begin with a letter, number, or the underscore character (_), and must consist only of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after epa action is created.The following requirement applies only to the Citrix ADC CLI:If the name includes one or

more spaces, enclose the name in double or single quotation marks (for example, "my aaa action" or 'my aaa action').

csecexpr it holds the ClientSecurityExpression to be sent to the client

killProcess String specifying the name of a process to be terminated by the endpoint analysis (EPA) tool. Multiple processes to be delimited by comma

deletefiles String specifying the path(s) and name(s) of the files to be deleted by the endpoint analysis (EPA) tool. Multiple files to be delimited by comma

defaultEPAGroup This is the default group that is chosen when the EPA check succeeds. Maximum value: 64

quarantineGroup This is the quarantine group that is chosen when the EPA check fails if configured. Maximum value: 64

authentication-ldapAction

The following operations can be performed on "authentication-ldapAction":

rm| add| show| set| unset|

rm authentication ldapAction

Removes an LDAP profile (action). NOTE: An action cannot be removed if it is bound to a policy.

Synopsis

rm authentication ldapAction <name>

Arguments

name Name of the LDAP profile (action) to be removed.

add authentication ldapAction

Creates an action (profile) for an LDAP server. This profile contains all configuration data needed to communicate with that LDAP server.

Synopsis

add authentication ldapAction <name> {-serverIP <ip_addr|ipv6_addr|*> | {-serverName <string>}} {-ldapBindDnPassword } [-nestedGroupExtraction (ON | OFF)] [-followReferrals (ON | OFF)] [-referralDNSLookup <referralDNSLookup>]

Arguments

name Name for the new LDAP action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the LDAP action is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication action" or 'my authentication action').

serverIP IP address assigned to the LDAP server.

serverName LDAP server name as a FQDN. Mutually exclusive with LDAP IP address.

serverPort Port on which the LDAP server accepts connections. Default value: 389 Minimum value: 1

authTimeout Number of seconds the Citrix ADC waits for a response from the RADIUS server. Default value: 3 Minimum value: 1

ldapBase Base (node) from which to start LDAP searches. If the LDAP server is running locally, the default value of base is dc=netscaler, dc=com.

ldapBindDn Full distinguished name (DN) that is used to bind to the LDAP server. Default: cn=Manager,dc=netscaler,dc=com

ldapBindDnPassword Password used to bind to the LDAP server.

ldapLoginName LDAP login name attribute. The Citrix ADC uses the LDAP login name to query external LDAP servers or Active Directories.

searchFilter String to be combined with the default LDAP user search string to form the search value. For example, if the search filter "vpnallowed=true" is combined with the LDAP login name "samaccount" and the user-supplied username is "bob", the result is the LDAP search string ""&(vpnallowed=true)(samaccount=bob)"" (Be sure to enclose the search string in two sets of double quotation marks; both sets are needed.).

groupAttrName LDAP group attribute name. Used for group extraction on the LDAP server.

subAttributeName LDAP group sub-attribute name. Used for group extraction from the LDAP server.

secType Type of security used for communications between the Citrix ADC and the LDAP server. For the PLAINTEXT setting, no encryption is required.

Possible values: PLAINTEXT, TLS, SSL Default value: PLAINTEXT

svrType The type of LDAP server.

Possible values: AD, NDS Default value: AAA_LDAP_SERVER_TYPE_DEFAULT

ssoNameAttribute LDAP single signon (SSO) attribute. The Citrix ADC uses the SSO name attribute to query external LDAP servers or Active Directories for an alternate username.

authentication Perform LDAP authentication. If authentication is disabled, any LDAP authentication attempt returns authentication success if the user is found. CAUTION! Authentication should be disabled only for authorization group extraction or where other (non-LDAP) authentication methods are in use and either bound to a primary list or flagged as secondary.

Possible values: ENABLED, DISABLED Default value: ENABLED

requireUser Require a successful user search for authentication. CAUTION! This field should be set to NO only if usersearch not required and (non-LDAP) authentication methods are in use and either bound to a primary list or flagged as secondary.

Possible values: YES, NO Default value: YES

passwdChange Allow password change requests.

Possible values: ENABLED, DISABLED Default value: DISABLED

nestedGroupExtraction Allow nested group extraction, in which the Citrix ADC queries external LDAP servers to determine whether a group is part of another group.

Possible values: ON, OFF Default value: OFF

maxNestingLevel If nested group extraction is ON, specifies the number of levels up to which group extraction is performed. Default value: 2 Minimum value: 2

followReferrals Setting this option to ON enables following LDAP referrals received from the LDAP server.

Possible values: ON, OFF Default value: OFF

maxLDAPReferrals Specifies the maximum number of nested referrals to follow. Default value: 1 Minimum value: 1

referralDNSLookup Specifies the DNS Record lookup Type for the referrals

Possible values: A-REC, SRV-REC, MSSRV-REC Default value: A-REC

msSRVRecordlocation MSSRV Specific parameter. Used to locate the DNS node to which the SRV record pertains in the domainname. The domainname is appended to it to form the srv record. Example : For "dc._msdcs", the srv record formed is _ldap._tcp.dc._msdcs.<domainname>. Default value: NS_S_DEFAULT_MSSRV_RECORDLOCATION

validateServerCert When to validate LDAP server certs

Possible values: YES, NO Default value: NO

ldapHostname Hostname for the LDAP server. If -validateServerCert is ON then this must be the host name on the certificate from the LDAP server. A hostname mismatch will cause a connection failure.

groupNameIdentifier Name that uniquely identifies a group in LDAP or Active Directory.

groupSearchAttribute LDAP group search attribute. Used to determine to which groups a group belongs.

groupSearchSubAttribute LDAP group search subattribute. Used to determine to which groups a group belongs.

groupSearchFilter String to be combined with the default LDAP group search string to form the search value. For example, the group search filter ""vpnallowed=true"" when combined with the group identifier ""samaccount"" and the group name ""g1"" yields the LDAP search string ""(&(vpnallowed=true)(samaccount=g1)"". If nestedGroupExtraction is ENABLED, the filter is applied on the first level group search as well, otherwise first level groups (of which user is a direct member of) will be fetched without applying this filter. (Be sure to enclose the search string in two sets of double quotation marks; both sets are needed.)

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

Attribute1 Expression that would be evaluated to extract attribute1 from the ldap response

Attribute2 Expression that would be evaluated to extract attribute2 from the ldap response

Attribute3 Expression that would be evaluated to extract attribute3 from the ldap response

Attribute4 Expression that would be evaluated to extract attribute4 from the ldap response

Attribute5 Expression that would be evaluated to extract attribute5 from the ldap response

Attribute6 Expression that would be evaluated to extract attribute6 from the ldap response

Attribute7 Expression that would be evaluated to extract attribute7 from the ldap response

Attribute8 Expression that would be evaluated to extract attribute8 from the ldap response

Attribute9 Expression that would be evaluated to extract attribute9 from the ldap response

Attribute10 Expression that would be evaluated to extract attribute10 from the ldap response

Attribute11 Expression that would be evaluated to extract attribute11 from the ldap response

Attribute12 Expression that would be evaluated to extract attribute12 from the ldap response

Attribute13 Expression that would be evaluated to extract attribute13 from the ldap response

Attribute14 Expression that would be evaluated to extract attribute14 from the ldap response

Attribute15 Expression that would be evaluated to extract attribute15 from the ldap response

Attribute16 Expression that would be evaluated to extract attribute16 from the ldap response

Attributes List of attribute names separated by ',' which needs to be fetched from ldap server. Note that preceeding and trailing spaces will be removed. Attribute name can be 127 bytes and total length of this string should not cross 2047 bytes. These attributes have multi-value support separated by ',' and stored as key-value pair in AAA session

sshPublicKey SSH PublicKey is attribute on AD. This attribute is used to retrieve ssh PublicKey for RBA authentication

pushService Name of the service used to send push notifications

OTPSecret OneTimePassword(OTP) Secret key attribute on AD. This attribute is used to store and retrieve secret key used for OTP check

email The Citrix ADC uses the email attribute to query the Active Directory for the email id of a user Default value: mail

KBAttribute KnowledgeBasedAuthentication(KBA) attribute on AD. This attribute is used to store and retrieve preconfigured Question and Answer knowledge base used for KBA authentication.

alternateEmailAttr The NetScaler appliance uses the alternateive email attribute to query the Active Directory for the alternative email id of a user

CloudAttributes The Citrix ADC uses the cloud attributes to extract additional attributes from LDAP servers required for Citrix Cloud operations

Possible values: ENABLED, DISABLED Default value: DISABLED

show authentication ldapAction

Displays the current configuration settings for the specified LDAP profile (action).

Synopsis

show authentication ldapAction

Arguments

name Name of the LDAP profile.

Output

serverIP IP address assigned to the LDAP server.

serverName LDAP server name as a FQDN. Mutually exclusive with LDAP IP address.

serverPort Port on which the LDAP server accepts connections.

authTimeout Number of seconds the Citrix ADC waits for a response from the RADIUS server.

ldapBindDn Full distinguished name (DN) that is used to bind to the LDAP server. Default: cn=Manager,dc=netscaler,dc=com

ldapBindDnPassword Password used to bind to the LDAP server.

ldapLoginName LDAP login name attribute. The Citrix ADC uses the LDAP login name to query external LDAP servers or Active Directories.

ldapBase Base (node) from which to start LDAP searches. If the LDAP server is running locally, the default value of base is dc=netscaler, dc=com.

searchFilter String to be combined with the default LDAP user search string to form the search value. For example, if the search filter "vpnallowed=true" is combined with the LDAP login name "samaccount" and the user-supplied username is "bob", the result is the LDAP search string ""&(vpnallowed=true)(samaccount=bob)"" (Be sure to enclose the search string in two sets of double quotation marks; both sets are needed.).

groupAttrName LDAP group attribute name. Used for group extraction on the LDAP server.

subAttributeName LDAP group sub-attribute name. Used for group extraction from the LDAP server.

secType Type of security used for communications between the Citrix ADC and the LDAP server. For the PLAINTEXT setting, no encryption is required.

svrType The type of LDAP server.

ssoNameAttribute LDAP single signon (SSO) attribute. The Citrix ADC uses the SSO name attribute to query external LDAP servers or Active Directories for an alternate username.

authentication Perform LDAP authentication. If authentication is disabled, any LDAP authentication attempt returns authentication success if the user is found. CAUTION! Authentication should be disabled only for authorization group extraction or where other (non-LDAP) authentication methods are in use and either bound to a primary list or flagged as secondary.

requireUser Require a successful user search for authentication. CAUTION! This field should be set to NO only if usersearch not required and (non-LDAP) authentication methods are in use and either bound to a primary list or flagged as secondary.

Success Failure stateflag nestedGroupExtraction Allow nested group extraction, in which the Citrix ADC queries external LDAP servers to determine whether a group is part of another group.

maxNestingLevel If nested group extraction is ON, specifies the number of levels up to which group extraction is performed.

followReferrals Setting this option to ON enables following LDAP referrals received from the LDAP server.

maxLDAPReferrals Specifies the maximum number of nested referrals to follow.

referralDNSLookup Specifies the DNS Record lookup Type for the referrals

msSRVRecordlocation MSSRV Specific parameter. Used to locate the DNS node to which the SRV record pertains in the domainname. The domainname is appended to it to form the srv record. Example : For "dc._msdcs", the srv record formed is _ldap._tcp.dc._msdcs.<domainname>.

validateServerCert When to validate LDAP server certs

ldapHostname Hostname for the LDAP server. If -validateServerCert is ON then this must be the host name on the certificate from the LDAP server. A hostname mismatch will cause a connection failure.

groupNameIdentifier Name that uniquely identifies a group in LDAP or Active Directory.

groupSearchAttribute LDAP group search attribute. Used to determine to which groups a group belongs.

groupSearchSubAttribute LDAP group search subattribute. Used to determine to which groups a group belongs.

groupSearchFilter String to be combined with the default LDAP group search string to form the search value. For example, the group search filter ""vpnallowed=true"" when combined with the group identifier ""samaccount"" and the group name ""g1"" yields the LDAP search string ""(&(vpnallowed=true)(samaccount=g1)"". If nestedGroupExtraction is ENABLED, the filter is applied on the first level group search as well, otherwise first level groups (of which user is a direct member of) will be fetched without applying this filter. (Be sure to enclose the search string in two sets of double quotation marks; both sets are needed.)

passwdChange Allow password change requests.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

Attribute1 Expression that would be evaluated to extract attribute1 from the ldap response

Attribute2 Expression that would be evaluated to extract attribute2 from the ldap response

Attribute3 Expression that would be evaluated to extract attribute3 from the ldap response

Attribute4 Expression that would be evaluated to extract attribute4 from the ldap response

Attribute5 Expression that would be evaluated to extract attribute5 from the ldap response

Attribute6 Expression that would be evaluated to extract attribute6 from the ldap response

Attribute7 Expression that would be evaluated to extract attribute7 from the ldap response

Attribute8 Expression that would be evaluated to extract attribute8 from the ldap response

Attribute9 Expression that would be evaluated to extract attribute9 from the ldap response

Attribute10 Expression that would be evaluated to extract attribute10 from the ldap response

Attribute11 Expression that would be evaluated to extract attribute11 from the ldap response

Attribute12 Expression that would be evaluated to extract attribute12 from the ldap response

Attribute13 Expression that would be evaluated to extract attribute13 from the ldap response

Attribute14 Expression that would be evaluated to extract attribute14 from the ldap response

Attribute15 Expression that would be evaluated to extract attribute15 from the ldap response

Attribute16 Expression that would be evaluated to extract attribute16 from the ldap response

Attributes List of attribute names separated by ',' which needs to be fetched from ldap server. Note that preceeding and trailing spaces will be removed. Attribute name can be 127 bytes and total length of this string should not cross 2047 bytes. These attributes have multi-value support separated by ',' and stored as key-value pair in AAA session

OTPSecret OneTimePassword(OTP) Secret key attribute on AD. This attribute is used to store and retrieve secret key used for OTP check

sshPublicKey SSH PublicKey is attribute on AD. This attribute is used to retrieve ssh PublicKey for RBA authentication

pushService Name of the service used to send push notifications

email The Citrix ADC uses the email attribute to query the Active Directory for the email id of a user

KBAttribute KnowledgeBasedAuthentication(KBA) attribute on AD. This attribute is used to store and retrieve preconfigured Question and Answer knowledge base used for KBA authentication.

alternateEmailAttr The NetScaler appliance uses the alternateive email attribute to query the Active Directory for the alternative email id of a user

CloudAttributes The Citrix ADC uses the cloud attributes to extract additional attributes from LDAP servers required for Citrix Cloud operations

devno count

set authentication ldapAction

Modifies an LDAP server profile (action.) The profile contains all configuration data needed to communicate with that LDAP server.

Synopsis

set authentication ldapAction <name> {-ldapBindDnPassword } [-groupSearchAttribute <string>]

Arguments

name Name of the LDAP profile to modify.

serverIP IP address assigned to the LDAP server.

serverName LDAP server name as a FQDN. Mutually exclusive with LDAP IP address.

serverPort Port on which the LDAP server accepts connections. Default value: 389 Minimum value: 1

authTimeout Number of seconds the Citrix ADC waits for a response from the RADIUS server. Default value: 3 Minimum value: 1

ldapBase Base (node) from which to start LDAP searches. If the LDAP server is running locally, the default value of base is dc=netscaler, dc=com.

ldapBindDn Full distinguished name (DN) that is used to bind to the LDAP server. Default: cn=Manager,dc=netscaler,dc=com

ldapBindDnPassword Password used to bind to the LDAP server.

ldapLoginName LDAP login name attribute. The Citrix ADC uses the LDAP login name to query external LDAP servers or Active Directories.

searchFilter String to be combined with the default LDAP user search string to form the search value. For example, if the search filter "vpnallowed=true" is combined with the LDAP login name "samaccount" and the user-supplied username is "bob", the result is the LDAP search string ""'&(vpnallowed=true)(samaccount=bob)"" (Be sure to enclose the search string in two sets of double quotation marks; both sets are needed.).

groupAttrName LDAP group attribute name. Used for group extraction on the LDAP server.

subAttributeName LDAP group sub-attribute name. Used for group extraction from the LDAP server.

secType Type of security used for communications between the Citrix ADC and the LDAP server. For the PLAINTEXT setting, no encryption is required.

Possible values: PLAINTEXT, TLS, SSL Default value: PLAINTEXT

svrType The type of LDAP server.

Possible values: AD, NDS Default value: AAA_LDAP_SERVER_TYPE_DEFAULT

ssoNameAttribute LDAP single signon (SSO) attribute. The Citrix ADC uses the SSO name attribute to query external LDAP servers or Active Directories for an alternate username.

authentication Perform LDAP authentication. If authentication is disabled, any LDAP authentication attempt returns authentication success if the user is found. CAUTION! Authentication should be disabled only for authorization group extraction or where other (non-LDAP) authentication methods are in use and either bound to a primary list or flagged as secondary.

Possible values: ENABLED, DISABLED Default value: ENABLED

requireUser Require a successful user search for authentication. CAUTION! This field should be set to NO only if usersearch not required and (non-LDAP) authentication methods are in use and either bound to a primary list or flagged as secondary.

Possible values: YES, NO Default value: YES

passwdChange Allow password change requests.

Possible values: ENABLED, DISABLED Default value: DISABLED

validateServerCert When to validate LDAP server certs

Possible values: YES, NO Default value: NO

ldapHostname Hostname for the LDAP server. If -validateServerCert is ON then this must be the host name on the certificate from the LDAP server. A hostname mismatch will cause a connection failure.

nestedGroupExtraction Allow nested group extraction, in which the Citrix ADC queries external LDAP servers to determine whether a group is part of another group.

Possible values: ON, OFF Default value: OFF

maxNestingLevel If nested group extraction is ON, specifies the number of levels up to which group extraction is performed. Default value: 2 Minimum value: 2

groupNameIdentifier Name that uniquely identifies a group in LDAP or Active Directory.

groupSearchAttribute LDAP group search attribute. Used to determine to which groups a group belongs.

groupSearchSubAttribute LDAP group search subattribute. Used to determine to which groups a group belongs.

groupSearchFilter String to be combined with the default LDAP group search string to form the search value. For example, the group search filter ""vpnallowed=true"" when combined with the group identifier ""samaccount"" and the group name ""g1"" yields the LDAP search string ""(&(vpnallowed=true)(samaccount=g1)"". If nestedGroupExtraction is ENABLED, the filter is applied on the first level group search as well, otherwise first level groups (of which user is a direct member of) will be fetched without applying this filter. (Be sure to enclose the search string in two sets of double quotation marks; both sets are needed.)

followReferrals Setting this option to ON enables following LDAP referrals received from the LDAP server.

Possible values: ON, OFF Default value: OFF

maxLDAPReferrals Specifies the maximum number of nested referrals to follow. Default value: 1 Minimum value: 1

referralDNSLookup Specifies the DNS Record lookup Type for the referrals

Possible values: A-REC, SRV-REC, MSSRV-REC Default value: A-REC

msSRVRecordlocation MSSRV Specific parameter. Used to locate the DNS node to which the SRV record pertains in the domainname. The domainname is appended to it to form the srv record. Example : For "dc._msdcs", the srv record formed is _ldap._tcp.dc._msdcs.<domainname>. Default value: NS_S_DEFAULT_MSSRV_RECORDLOCATION

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

Attribute1 Expression that would be evaluated to extract attribute1 from the ldap response

Attribute2 Expression that would be evaluated to extract attribute2 from the ldap response

Attribute3 Expression that would be evaluated to extract attribute3 from the ldap response

Attribute4 Expression that would be evaluated to extract attribute4 from the ldap response

Attribute5 Expression that would be evaluated to extract attribute5 from the ldap response

Attribute6 Expression that would be evaluated to extract attribute6 from the ldap response

Attribute7 Expression that would be evaluated to extract attribute7 from the ldap response

Attribute8 Expression that would be evaluated to extract attribute8 from the ldap response

Attribute9 Expression that would be evaluated to extract attribute9 from the ldap response

Attribute10 Expression that would be evaluated to extract attribute10 from the ldap response

Attribute11 Expression that would be evaluated to extract attribute11 from the ldap response

Attribute12 Expression that would be evaluated to extract attribute12 from the ldap response

Attribute13 Expression that would be evaluated to extract attribute13 from the ldap response

Attribute14 Expression that would be evaluated to extract attribute14 from the ldap response

Attribute15 Expression that would be evaluated to extract attribute15 from the ldap response

Attribute16 Expression that would be evaluated to extract attribute16 from the ldap response

Attributes List of attribute names separated by ',' which needs to be fetched from ldap server. Note that preceeding and trailing spaces will be removed. Attribute name can be 127 bytes and total length of this string should not cross 2047 bytes. These attributes have multi-value support separated by ',' and stored as key-value pair in AAA session

OTPSecret OneTimePassword(OTP) Secret key attribute on AD. This attribute is used to store and retrieve secret key used for OTP check

sshPublicKey SSH PublicKey is attribute on AD. This attribute is used to retrieve ssh PublicKey for RBA authentication

pushService Name of the service used to send push notifications

email The Citrix ADC uses the email attribute to query the Active Directory for the email id of a user Default value: mail

KBAttribute KnowledgeBasedAuthentication(KBA) attribute on AD. This attribute is used to store and retrieve preconfigured Question and Answer knowledge base used for KBA authentication.

alternateEmailAttr The NetScaler appliance uses the alternateive email attribute to query the Active Directory for the alternative email id of a user

CloudAttributes The Citrix ADC uses the cloud attributes to extract additional attributes from LDAP servers required for Citrix Cloud operations

Possible values: ENABLED, DISABLED Default value: DISABLED

unset authentication ldapAction

Use this command to remove authentication ldapAction settings.Refer to the set authentication ldapAction command for meanings of the arguments.

Synopsis

unset authentication ldapAction <name>

authentication-ldapPolicy

The following operations can be performed on "authentication-ldapPolicy":

set| show| rm| add| unset|

set authentication ldapPolicy

Configures the specified LDAP policy.

Synopsis

set authentication ldapPolicy <name>

Arguments

name Name of the LDAP policy.

rule The new rule to associate with the policy.

reqAction The new LDAP action to associate with the policy.

show authentication ldapPolicy

Displays the current settings for the specified LDAP policy. If no policy name is provided, displays a list of all LDAP policies currently configured on the Citrix ADC.

Synopsis

show authentication ldapPolicy

Arguments

name Name of the LDAP policy.

Output

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the LDAP server.

reqAction Name of the LDAP action to perform if the policy matches.

boundTo The entity name to which policy is bound

activePolicy priority bindPolicyType policyType devno count stateflag

rm authentication ldapPolicy

Removes an LDAP policy.

Synopsis

rm authentication ldapPolicy <name>

Arguments

name Name of the LDAP policy to remove.

add authentication ldapPolicy

Adds an LDAP authentication policy. The policy defines the criteria under which the Citrix ADC attempts to authenticate the user with the specified LDAP server.

Synopsis

add authentication ldapPolicy <name> <rule>

Arguments

name Name for the LDAP policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after LDAP policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the LDAP server.

reqAction Name of the LDAP action to perform if the policy matches.

unset authentication ldapPolicy

Use this command to remove authentication ldapPolicy settings.Refer to the set authentication ldapPolicy command for meanings of the arguments.

Synopsis

unset authentication ldapPolicy <name>

authentication-localPolicy

The following operations can be performed on "authentication-localPolicy":

add| show| rm| set|

add authentication localPolicy

Adds a policy for the Citrix ADC to locally authenticate a user. The policy contains criteria that specify when and how to authenticate a user.

Synopsis

add authentication localPolicy <name> <rule>

Arguments

name Name for the local authentication policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#),

space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after local policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to perform the authentication.

show authentication localPolicy

Displays the current settings for the specified local authentication policy. If no policy name is provided, displays a list of all local authentication policies currently configured on the Citrix ADC.

Synopsis

show authentication localPolicy

Arguments

name Name of the local authentication policy.

Output

rule The new rule associated with the policy.

boundTo The entity name to which policy is bound

activePolicy priority reqAction The name of the RADIUS action the policy uses

bindPolicyType policyType devno count stateflag

rm authentication localPolicy

Removes the specified local authentication policy.

Synopsis

rm authentication localPolicy <name>

Arguments

name Name of the local policy to remove.

set authentication localPolicy

Configures the specified local authentication policy.

Synopsis

set authentication localPolicy <name> -rule <expression>

Arguments

name Name of the local authentication policy.

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to perform the authentication.

authentication-loginSchema

The following operations can be performed on "authentication-loginSchema":

unset| add| show| rm| set|

unset authentication loginSchema

Use this command to remove authentication loginSchema settings.Refer to the set authentication loginSchema command for meanings of the arguments.

Synopsis

unset authentication loginSchema <name>

add authentication loginSchema

Creates a LoginSchema. This profile is used to send authentication requirements to the UI tier for login

Synopsis

add authentication loginSchema <name> -authenticationSchema <string>

Arguments

name Name for the new login schema. Login schema defines the way login form is rendered. It provides a way to customize the fields that are shown to the user. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore,

hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

authenticationSchema Name of the file for reading authentication schema to be sent for Login Page UI. This file should contain xml definition of elements as per Citrix Forms Authentication Protocol to be able to render login form. If administrator does not want to prompt users for additional credentials but continue with previously obtained credentials, then "noschema" can be given as argument. Please note that this applies only to loginSchemas that are used with user-defined factors, and not the vserver factor.

userExpression Expression for username extraction during login. This can be any relevant advanced policy expression.

passwdExpression Expression for password extraction during login. This can be any relevant advanced policy expression.

userCredentialIndex The index at which user entered username should be stored in session. Minimum value: 1 Maximum value: 16

passwordCredentialIndex The index at which user entered password should be stored in session. Minimum value: 1 Maximum value: 16

authenticationStrength Weight of the current authentication Minimum value: 0 Maximum value: 65535

SSOCredentials This option indicates whether current factor credentials are the default SSO (SingleSignOn) credentials.

Possible values: YES, NO Default value: NO

show authentication loginSchema

Displays information about all configured login schema, or displays detailed information about the specified schema.

Synopsis

show authentication loginSchema

Arguments

name Name for the new login schema. Login schema defines the way login form is rendered. It provides a way to customize the fields that are shown to the user. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

Output

authenticationSchema Name of the file for reading authentication schema to be sent for Login Page UI. This file should contain xml definition of elements as per Citrix Forms Authentication Protocol to be able to render login form. If administrator does not want to prompt users for additional credentials but continue with previously obtained credentials, then "noschema" can be given as argument. Please note that this applies only to loginSchemas that are used with user-defined factors, and not the vserver factor.

userExpression Expression for username extraction during login. This can be any relevant advanced policy expression.

passwdExpression Expression for password extraction during login. This can be any relevant advanced policy expression.

userCredentialIndex The index at which user entered username should be stored in session.

passwordCredentialIndex The index at which user entered password should be stored in session.

authenticationStrength Weight of the current authentication

SSOCredentials This option indicates whether current factor credentials are the default SSO (SingleSignOn) credentials.

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

devno count stateflag

rm authentication loginSchema

Deletes an existing LoginSchema.

Synopsis

rm authentication loginSchema <name>

Arguments

name Name for the new login schema. Login schema defines the way login form is rendered. It provides a way to customize the fields that are shown to the user. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

set authentication loginSchema

Modifies the specified attributes of a LoginSchema.

Synopsis

set authentication loginSchema <name>

Arguments

name Name for the new login schema. Login schema defines the way login form is rendered. It provides a way to customize the fields that are shown to the user. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

authenticationSchema Name of the file for reading authentication schema to be sent for Login Page UI. This file should contain xml definition of elements as per Citrix Forms Authentication Protocol to be able to render login form. If administrator does not want to prompt users for additional credentials but continue with previously obtained credentials, then "noschema" can be

given as argument. Please note that this applies only to loginSchemas that are used with user-defined factors, and not the vserver factor.

userExpression Expression for username extraction during login. This can be any relevant advanced policy expression.

passwdExpression Expression for password extraction during login. This can be any relevant advanced policy expression.

userCredentialIndex The index at which user entered username should be stored in session. Minimum value: 1 Maximum value: 16

passwordCredentialIndex The index at which user entered password should be stored in session. Minimum value: 1 Maximum value: 16

authenticationStrength Weight of the current authentication Minimum value: 0 Maximum value: 65535

SSOCredentials This option indicates whether current factor credentials are the default SSO (SingleSignOn) credentials.

Possible values: YES, NO Default value: NO

authentication-loginSchemaPolicy

The following operations can be performed on "authentication-loginSchemaPolicy":

set| rm| unset| rename| add| show| stat|

set authentication loginSchemaPolicy

Modifies the specified parameters of an existing policy.

Synopsis

set authentication loginSchemaPolicy <name>

Arguments

name Name of the policy to modify.

rule Expression which is evaluated to choose a profile for authentication.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the profile to apply to requests or connections that match this policy.

- NOOP - Do not take any specific action when this policy evaluates to true. This is useful to implicitly go to a different policy set.
- RESET - Reset the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend the request if desired.
- DROP - Drop the request without sending a response to the user.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

comment Any comments to preserve information about this policy.

logAction Name of messagelog action to use when a request matches this policy.

rm authentication loginSchemaPolicy

Removes an existing LoginSchema policy.

Synopsis

rm authentication loginSchemaPolicy <name>

Arguments

name Name of the policy to remove.

unset authentication loginSchemaPolicy

Removes the settings of an existing policy. Attributes for which a default value is available revert to their default values. See the set LoginSchemaPolicy command for a description of the parameters..Refer to the set authentication loginSchemaPolicy command for meanings of the arguments.

Synopsis

unset authentication loginSchemaPolicy <name>

Example

unset LoginSchemaPolicy pol9 -undefAction

rename authentication loginSchemaPolicy

Renames the specified LoginSchema policy.

Synopsis

rename authentication loginSchemaPolicy <name>@ <newName>@

Arguments

name Existing name of the LoginSchema policy.

newName New name for the LoginSchema policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my loginschemapolicy policy" or 'my loginschemapolicy policy').

Example

rename loginschemapolicy oldname newname

add authentication loginSchemaPolicy

Adds a LoginSchema policy for use in login parameter selection.

Synopsis

add authentication loginSchemaPolicy <name> -rule <expression> -action <string>

Arguments

name Name for the LoginSchema policy. This is used for selecting parameters for user logon. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

rule Expression which is evaluated to choose a profile for authentication.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the profile to apply to requests or connections that match this policy.

- NOOP - Do not take any specific action when this policy evaluates to true. This is useful to implicitly go to a different policy set.
- RESET - Reset the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend the request if desired.
- DROP - Drop the request without sending a response to the user.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

comment Any comments to preserve information about this policy.

logAction Name of messagelog action to use when a request matches this policy.

show authentication loginSchemaPolicy

Displays information about all configured LoginSchema policies, or displays detailed information about the specified policy.

Synopsis

show authentication loginSchemaPolicy

Arguments

name Name of the LoginSchema policy for which to display detailed information.

Output

rule The rule used by the LoginSchema authentication policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide

action The action to be performed when the rule is matched.

stateflag undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

comment Any comments to preserve information about this policy.

logAction Name of messagelog action to use when a request matches this policy.

boundTo The entity name to which policy is bound

activePolicy priority gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

hits Number of hits.

bindPolicyType vserverType undefHits Number of Undef hits.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

builtin Flag to determine if policy is built-in or not

feature The feature to be checked while applying this config

devno count

stat authentication loginSchemaPolicy

Display LoginSchema policy statistics.

Synopsis

stat authentication loginSchemaPolicy

Arguments

name The name of the LoginSchema policy for which statistics will be displayed. If not given statistics are shown for all policies.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Policy undef hits (Undefhits) Number of undef hits on the policy

Example

stat authentication loginschemapolicy.

Related Commands

- stat authentication OAuthIdPPolicy

authentication-negotiateAction

The following operations can be performed on "authentication-negotiateAction":

set| show| add| unset| rm|

set authentication negotiateAction

Configures an AD KDC server profile (negotiate action).

Synopsis

set authentication negotiateAction <name>

Arguments

name Name of the AD KDC server profile.

domain Domain name of the service principal that represnts Citrix ADC.

domainUser User name of the account that is mapped with Citrix ADC principal. This can be given along with domain and password when keytab file is not available. If username is given along with keytab file, then that keytab file will be searched for this user's credentials.

domainUserPasswd Password of the account that is mapped to the Citrix ADC principal.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

keytab The path to the keytab file that is used to decrypt kerberos tickets presented to Citrix ADC. If keytab is not available, domain/username/password can be specified in the negotiate action configuration

NTLMPath The path to the site that is enabled for NTLM authentication, including FQDN of the server. This is used when clients fallback to NTLM.

show authentication negotiateAction

Displays the current configuration settings for the specified AD KDC server profile (negotiate action).

Synopsis

show authentication negotiateAction

Arguments

name Name of the AD KDC server profile.

Output

domain Domain name of the service principal that represnts Citrix ADC.

domainUser User name of the account that is mapped with Citrix ADC principal. This can be given along with domain and password when keytab file is not available. If username is given along with keytab file, then that keytab file will be searched for this user's credentials.

domainUserPasswd Password of the account that is mapped to the Citrix ADC principal.

OU Active Directory organizational units (OU) attribute.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

keytab The path to the keytab file that is used to decrypt kerberos tickets presented to Citrix ADC. If keytab is not available, domain/username/password can be specified in the negotiate action configuration

kcdSPN Host SPN extracted from keytab file.

NTLMPath The path to the site that is enabled for NTLM authentication, including FQDN of the server. This is used when clients fallback to NTLM.

stateflag devno count

add authentication negotiateAction

Creates an action (profile) for an Active Directory (AD) server that is used as a Kerberos Key Distribution Center (KDC). The profile contains all configuration data necessary to communicate with that AD KDC server.

Synopsis

add authentication negotiateAction <name> {-domain <string>} {-domainUser <string>} {-domainUserPasswd }

Arguments

name Name for the AD KDC server profile (negotiate action). Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after AD KDC server profile is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication action" or 'my authentication action').

domain Domain name of the service principal that represnts Citrix ADC.

domainUser User name of the account that is mapped with Citrix ADC principal. This can be given along with domain and password when keytab file is not available. If username is given along with keytab file, then that keytab file will be searched for this user's credentials.

domainUserPasswd Password of the account that is mapped to the Citrix ADC principal.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

keytab The path to the keytab file that is used to decrypt kerberos tickets presented to Citrix ADC. If keytab is not available, domain/username/password can be specified in the negotiate action configuration

NTLMPath The path to the site that is enabled for NTLM authentication, including FQDN of the server. This is used when clients fallback to NTLM.

unset authentication negotiateAction

Use this command to remove authentication negotiateAction settings.Refer to the set authentication negotiateAction command for meanings of the arguments.

Synopsis

unset authentication negotiateAction <name>

rm authentication negotiateAction

Removes an AD KDC server profile (negotiate action). An action cannot be removed if it is bound to a policy.

Synopsis

rm authentication negotiateAction <name>

Arguments

name Name of the AD KDC server profile to be removed.

authentication-negotiatePolicy

The following operations can be performed on "authentication-negotiatePolicy":

add| rm| set| show|

add authentication negotiatePolicy

Adds an Active Directory (AD) Kerberos Key Distribution Center (KCD) authentication policy (negotiate policy). The policy defines the criteria under which the Citrix ADC attempts to authenticate the user with the specified AD KCD server.

Synopsis

add authentication negotiatePolicy <name> <rule> <reqAction>

Arguments

name Name for the negotiate authentication policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after AD KCD (negotiate) policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the AD KCD server.

reqAction Name of the negotiate action to perform if the policy matches.

rm authentication negotiatePolicy

Removes the specified AD KCD (negotiate) policy.

Synopsis

rm authentication negotiatePolicy <name>

Arguments

name Name of the negotiate policy to remove.

set authentication negotiatePolicy

Modifies the specified AD KCD (negotiate) policy.

Synopsis

set authentication negotiatePolicy <name>

Arguments

name Name of the negotiate policy to modify.

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the AD KCD server.

reqAction Name of the negotiate action to perform if the policy matches.

show authentication negotiatePolicy

Displays the current settings for the specified AD KCD (negotiate) policy. If no policy name is provided, displays a list of all negotiate policies currently configured on the Citrix ADC.

Synopsis

show authentication negotiatePolicy

Arguments

name Name of the negotiate policy.

Output

rule The name of the new rule associated with the policy.

reqAction The name of the Negotiate action associated with the policy.

boundTo The entity name to which policy is bound

activePolicy priority bindPolicyType policyType devno count stateflag

authentication-noAuthAction

The following operations can be performed on "authentication-noAuthAction":

set| unset| add| show| rm|

set authentication noAuthAction

Modifies the specified attributes of an noauth action.

Synopsis

set authentication noAuthAction <name> -defaultAuthenticationGroup <string>

Arguments

name Name for the new no-authentication action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

defaultAuthenticationGroup This is the group that is added to user sessions that match current policy.

unset authentication noAuthAction

Use this command to remove authentication noAuthAction settings.Refer to the set authentication noAuthAction command for meanings of the arguments.

Synopsis

unset authentication noAuthAction <name> -defaultAuthenticationGroup

add authentication noAuthAction

Creates a noauth action. This action implies implicit success and inherits the default group. It could be used to craft policy decisions by giving default group.

Synopsis

add authentication noAuthAction <name>

Arguments

name Name for the new no-authentication action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

defaultAuthenticationGroup This is the group that is added to user sessions that match current policy.

show authentication noAuthAction

Displays information about all configured actions, or displays detailed information about the specified action.

Synopsis

show authentication noAuthAction

Arguments

name Name for the new no-authentication action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

Output

defaultAuthenticationGroup This is the group that is added to user sessions that match current policy.

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

devno count stateflag

rm authentication noAuthAction

Deletes an existing noauth action.

Synopsis

rm authentication noAuthAction <name>

Arguments

name Name for the new no-authentication action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

authentication-policylabel

The following operations can be performed on "authentication-policylabel":

rm| add| bind| show| unbind| stat| rename|

rm authentication policylabel

Removes an authorization policy label.

Synopsis

rm authentication policylabel <labelName>

Arguments

labelName Name of the authorization policy label to remove.

Example

rm authorization policylabel trans_http_url

add authentication policylabel

Creates a user-defined authentication policy label.

Synopsis

add authentication policylabel <labelName>

Arguments

labelName Name for the new authentication policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy label" or 'authentication policy label').

type Type of feature (aaatm or rba) against which to match the policies bound to this policy label.

Possible values: AAATM_REQ, RBA_REQ Default value: AAATM_REQ

comment Any comments to preserve information about this authentication policy label.

loginSchema Login schema associated with authentication policy label. Login schema defines the UI rendering by providing customization option of the fields. If user intervention is not needed for a given factor such as group extraction, a loginSchema whose authentication schema is "noschema" should be used.

Example

add authentication policylabel trans_http_url

bind authentication policylabel

Binds an authentication policy to .

Synopsis

bind authentication policylabel <labelName> -policyName <string> -priority <positive_integer>

Arguments

labelName Name of the authentication policy label to which to bind the policy.

policyName Name of the authentication policy to bind to the policy label.

priority Positive integer specifying the priority of the policy. The lower the number, the higher the priority. Policies within a label are evaluated in the order of their priority numbers. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.

- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is smaller than the current policy's priority number.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

nextFactor On success invoke label.

Example

i)bind authentication policylabel authn_label_1 -policyName authn_pol_1 -priority 1 ii)bind authentication policylabel authn_label_2 -policyName authn_pol_2 -priority 2 -nextFactor authn_label_1 -gotoPriorityExpression next

show authentication policylabel

Displays the current settings for the specified authentication policy label. If no policy name is provided, displays a list of all authentication policy labels currently configured on the Citrix ADC.

Synopsis

show authentication policylabel

Arguments

labelName Name of the authorization policy label.

Output

stateflag numpol Number of polices bound to label.

hits Number of times policy label was invoked.

policyName Name of the authentication policy to bind to the policy label.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

flowType Flowtype of the bound authentication policy.

description Description of the policylabel

flags nextFactor On success invoke label.

comment Any comments to preserve information about this authentication policy label.

loginSchema Login schema associated with authentication policy label. Login schema defines the UI rendering by providing customization option of the fields. If user intervention is not needed for a given factor such as group extraction, a loginSchema whose authentication schema is "noschema" should be used.

type Type of feature (aaatm or rba) against which to match the policies bound to this policy label.

devno count

Example

i)show authentication policylabel trans_http_url ii)show authentication policylabel

unbind authentication policylabel

Unbinds the specified policy from the specified authorization policy label.

Synopsis

unbind authentication policylabel <labelName> -policyName <string>

Arguments

labelName Name for the new authentication policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy label" or 'authentication policy label').

policyName Name of the authentication policy to bind to the policy label.

priority Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind authorization policylabel trans_http_url pol_1

stat authentication policylabel

Displays statistics for the specified authentication policy label. If no authentication policy label is specified, displays a list of all authentication policy labels.

Synopsis

stat authentication policylabel

Arguments

labelName Name of the authentication policy label.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy Label Hits (Hits) Number of times policy label was invoked.

Related Commands

- stat authentication OAuthIdPPolicy

rename authentication policylabel

Rename a authn policy label.

Synopsis

rename authentication policylabel <labelName>@ <newName>@

Arguments

labelName The name of the auth policy label

newName The new name of the auth policy label

Example

rename authn policy label oldname newname

authentication-pushService

The following operations can be performed on "authentication-pushService":

rm| show| add| set| unset|

rm authentication pushService

Remove a push service entity on the Citrix ADC

Synopsis

rm authentication pushService <name>

Arguments

name Name of the push service

Example

rm authentication pushservice <name>

show authentication pushService

Displays all the configured push service entities in the system. If a name is specified, then only that entity is shown.

Synopsis

show authentication pushService

Arguments

name Name of the push service entity.

Output

namespace This is fully qualified domain name of the notification service in the cloud. If omitted, namespace defaults to https://mfa.cloud.com/

hubName Name of the hub within a namespace. This is used to classify different identities within a namespace.

serviceKey Key to be used to compute signature necessary for registering to notification service.

serviceKeyName Friendly name of the Key to be used to compute signature necessary for registering to notification service.

clientID Unique identity for communicating with Citrix Push server in cloud.

clientSecret Unique secret for communicating with Citrix Push server in cloud.

CustomerID Customer id/name of the account in cloud that is used to create clientid/secret pair.

CertEndpoint URL of the endpoint that contains JWKs (Json Web Key) for JWT (Json Web Token) verification. This is used at cloud instance that offers push service.

refreshInterval Interval at which certificates or idtoken is refreshed.

stateflag State flag

pushServiceStatus Describes status of push service.

trustService URL of the service that generates tokens for cloud access.

pushCloudServerStatus Describes status of the cloud service that does push.

signingKeyName Friendly name of the Key to be used to compute signature necessary for accessing notification service.

signingKey Key to be used to compute signature necessary for accessing notification service.

devno count

Example

show authentication pushservice

add authentication pushService

Add a new push service entity on the Citrix ADC. The Push service will be configured with well known pre-defined default values for Namespace (https://mfa.cloud.com/) and Trust Service (https://trust.citrixworkspacesapi.net/) endpoints

Synopsis

add authentication pushService <name>

Arguments

name Name for the push service. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after the profile is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my push service" or 'my push service').

clientID Unique identity for communicating with Citrix Push server in cloud.

clientSecret Unique secret for communicating with Citrix Push server in cloud.

CustomerID Customer id/name of the account in cloud that is used to create clientid/secret pair.

refreshInterval Interval at which certificates or idtoken is refreshed. Default value: 50 Minimum value: 0

Example

add authentication pushservice <name> -clientid <> -clientsecret <> -customerid <>

set authentication pushService

Set/modify push service entity values

Synopsis

set authentication pushService <name>

Arguments

name Name for the push service. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after the profile is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my push service" or 'my push service').

clientID Unique identity for communicating with Citrix Push server in cloud.

clientSecret Unique secret for communicating with Citrix Push server in cloud.

CustomerID Customer id/name of the account in cloud that is used to create clientid/secret pair.

refreshInterval Interval at which certificates or idtoken is refreshed. Default value: 50 Minimum value: 0

Example

set authentication pushservice <profile name> -clientid <>

unset authentication pushService

Use this command to remove authentication pushService settings.Refer to the set authentication pushService command for meanings of the arguments.

Synopsis

unset authentication pushService <name> -refreshInterval

authentication-radiusAction

The following operations can be performed on "authentication-radiusAction":

set| unset| show| add| rm|

set authentication radiusAction

Configures a RADIUS server profile (action). The profile contains all configuration data needed to communicate with that RADIUS server.

Synopsis

set authentication radiusAction <name> {-radKey } [-transport <transport>]

Arguments

name Name of the RADIUS profile.

serverIP IP address assigned to the RADIUS server.

serverName RADIUS server name as a FQDN. Mutually exclusive with RADIUS IP address.

serverPort Port number on which the RADIUS server listens for connections. Minimum value: 1

authTimeout Number of seconds the Citrix ADC waits for a response from the RADIUS server. Default value: 3 Minimum value: 1

radKey Key shared between the RADIUS server and the Citrix ADC. Required to allow the Citrix ADC to communicate with the RADIUS server.

radNASip If enabled, the Citrix ADC IP address (NSIP) is sent to the RADIUS server as the Network Access Server IP (NASIP) address. The RADIUS protocol defines the meaning and use of the NASIP address.

Possible values: ENABLED, DISABLED

radNASid If configured, this string is sent to the RADIUS server as the Network Access Server ID (NASID).

radVendorID RADIUS vendor ID attribute, used for RADIUS group extraction. Minimum value: 1

radAttributeType RADIUS attribute type, used for RADIUS group extraction. Minimum value: 1

radGroupsPrefix RADIUS groups prefix string. This groups prefix precedes the group names within a RADIUS attribute for RADIUS group extraction.

radGroupSeparator RADIUS group separator string The group separator delimits group names within a RADIUS attribute for RADIUS group extraction.

passEncoding Encoding type for passwords in RADIUS packets that the Citrix ADC sends to the RADIUS server.

Possible values: pap, chap, mschapv1, mschapv2 Default value: pap

ipVendorID Vendor ID of the intranet IP attribute in the RADIUS response. NOTE: A value of 0 indicates that the attribute is not vendor encoded. Minimum value: 0

ipAttributeType Remote IP address attribute type in a RADIUS response. Minimum value: 1

accounting Whether the RADIUS server is currently accepting accounting messages.

Possible values: ON, OFF

pwdVendorID Vendor ID of the attribute, in the RADIUS response, used to extract the user password. Minimum value: 1

pwdAttributeType Vendor-specific password attribute type in a RADIUS response. Minimum value: 1

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

callingstationid Send Calling-Station-ID of the client to the RADIUS server. IP Address of the client is sent as its Calling-Station-ID.

Possible values: ENABLED, DISABLED Default value: DISABLED

authservRetry Number of retry by the Citrix ADC before getting response from the RADIUS server. Default value: 3 Minimum value: 1 Maximum value: 10

authentication Configure the RADIUS server state to accept or refuse authentication messages.

Possible values: ON, OFF Default value: ON

tunnelEndpointClientIP Send Tunnel Endpoint Client IP address to the RADIUS server.

Possible values: ENABLED, DISABLED Default value: DISABLED

transport Transport mode to RADIUS server.

Possible values: UDP, TCP, TLS Default value: RAD_TRANSPORT_UDP

targetLBVserver If transport mode is TLS, specify the name of LB vserver to associate. The LB vserver needs to be of type TCP and service associated needs to be SSL_TCP

Example

To modify an existing RADIUS Action with a different server running at say 10.217.201.20 and radkey set to newkey123: set authentication radiusAction radius_action -serverIP 10.217.201.20 -radKey newkey123

unset authentication radiusAction

Use this command to remove authentication radiusAction settings.Refer to the set authentication radiusAction command for meanings of the arguments.

Synopsis

unset authentication radiusAction <name>

show authentication radiusAction

Displays the current configuration settings for the specified RADIUS profile (action).

Synopsis

show authentication radiusAction

Arguments

name Name of the RADIUS profile.

Output

serverIP IP address assigned to the RADIUS server.

serverName RADIUS server name as a FQDN. Mutually exclusive with RADIUS IP address.

serverPort Port number on which the RADIUS server listens for connections.

authTimeout Number of seconds the Citrix ADC waits for a response from the RADIUS server.

radKey Key shared between the RADIUS server and the Citrix ADC. Required to allow the Citrix ADC to communicate with the RADIUS server.

radNASip If enabled, the Citrix ADC IP address (NSIP) is sent to the RADIUS server as the Network Access Server IP (NASIP) address. The RADIUS protocol defines the meaning and use of the NASIP address.

IPAddress IP address.

radNASid If configured, this string is sent to the RADIUS server as the Network Access Server ID (NASID).

radVendorID RADIUS vendor ID attribute, used for RADIUS group extraction.

radAttributeType RADIUS attribute type, used for RADIUS group extraction.

radGroupsPrefix RADIUS groups prefix string. This groups prefix precedes the group names within a RADIUS attribute for RADIUS group extraction.

radGroupSeparator RADIUS group separator string The group separator delimits group names within a RADIUS attribute for RADIUS group extraction.

passEncoding Encoding type for passwords in RADIUS packets that the Citrix ADC sends to the RADIUS server.

ipVendorID Vendor ID of the intranet IP attribute in the RADIUS response. NOTE: A value of 0 indicates that the attribute is not vendor encoded.

ipAttributeType Remote IP address attribute type in a RADIUS response.

accounting Whether the RADIUS server is currently accepting accounting messages.

Success Failure stateflag pwdVendorID Vendor ID of the attribute, in the RADIUS response, used to extract the user password.

pwdAttributeType Vendor-specific password attribute type in a RADIUS response.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

callingstationid Send Calling-Station-ID of the client to the RADIUS server. IP Address of the client is sent as its Calling-Station-ID.

authservRetry Number of retry by the Citrix ADC before getting response from the RADIUS server.

authentication Configure the RADIUS server state to accept or refuse authentication messages.

tunnelEndpointClientIP Send Tunnel Endpoint Client IP address to the RADIUS server.

transport Transport mode to RADIUS server.

targetLBVserver If transport mode is TLS, specify the name of LB vserver to associate. The LB vserver needs to be of type TCP and service associated needs to be SSL_TCP

devno count

Example

show authentication radiusaction radius_action

add authentication radiusAction

Creates an action (profile) for a RADIUS server. The profile contains all configuration data necessary to communicate with that RADIUS server.

Synopsis

add authentication radiusAction <name> {-serverIP <ip_addr|ipv6_addr|*> | {-serverName <string>}} {-radKey } [-pwdVendorID <positive_integer>] [-transport <transport>]

Arguments

name Name for the RADIUS action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the RADIUS action is added.

serverIP IP address assigned to the RADIUS server.

serverName RADIUS server name as a FQDN. Mutually exclusive with RADIUS IP address.

serverPort Port number on which the RADIUS server listens for connections. Minimum value: 1

authTimeout Number of seconds the Citrix ADC waits for a response from the RADIUS server. Default value: 3 Minimum value: 1

radKey Key shared between the RADIUS server and the Citrix ADC. Required to allow the Citrix ADC to communicate with the RADIUS server.

radNASip If enabled, the Citrix ADC IP address (NSIP) is sent to the RADIUS server as the Network Access Server IP (NASIP) address. The RADIUS protocol defines the meaning and use of the NASIP address.

Possible values: ENABLED, DISABLED

radNASid If configured, this string is sent to the RADIUS server as the Network Access Server ID (NASID).

radVendorID RADIUS vendor ID attribute, used for RADIUS group extraction. Minimum value: 1

radAttributeType RADIUS attribute type, used for RADIUS group extraction. Minimum value: 1

radGroupsPrefix RADIUS groups prefix string. This groups prefix precedes the group names within a RADIUS attribute for RADIUS group extraction.

radGroupSeparator RADIUS group separator string The group separator delimits group names within a RADIUS attribute for RADIUS group extraction.

passEncoding Encoding type for passwords in RADIUS packets that the Citrix ADC sends to the RADIUS server.

Possible values: pap, chap, mschapv1, mschapv2 Default value: pap

ipVendorID Vendor ID of the intranet IP attribute in the RADIUS response. NOTE: A value of 0 indicates that the attribute is not vendor encoded. Minimum value: 0

ipAttributeType Remote IP address attribute type in a RADIUS response. Minimum value: 1

accounting Whether the RADIUS server is currently accepting accounting messages.

Possible values: ON, OFF

pwdVendorID Vendor ID of the attribute, in the RADIUS response, used to extract the user password. Minimum value: 1

pwdAttributeType Vendor-specific password attribute type in a RADIUS response. Minimum value: 1

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

callingstationid Send Calling-Station-ID of the client to the RADIUS server. IP Address of the client is sent as its Calling-Station-ID.

Possible values: ENABLED, DISABLED Default value: DISABLED

authservRetry Number of retry by the Citrix ADC before getting response from the RADIUS server. Default value: 3 Minimum value: 1 Maximum value: 10

authentication Configure the RADIUS server state to accept or refuse authentication messages.

Possible values: ON, OFF Default value: ON

tunnelEndpointClientIP Send Tunnel Endpoint Client IP address to the RADIUS server.

Possible values: ENABLED, DISABLED Default value: DISABLED

transport Transport mode to RADIUS server.

Possible values: UDP, TCP, TLS Default value: RAD_TRANSPORT_UDP

targetLBVserver If transport mode is TLS, specify the name of LB vserver to associate. The LB vserver needs to be of type TCP and service associated needs to be SSL_TCP

Example

To Add a default RADIUS Action with server running at 10.217.201.10 and radkey set to testing123: add authentication radiusAction radius_action -serverIP 10.217.201.10 -radKey testing123

rm authentication radiusAction

Removes a RADIUS profile (action). An action cannot be removed as long as it is bound to a policy.

Synopsis

rm authentication radiusAction <name>

Arguments

name Name of the action to be removed.

Example

To remove a RADIUS Action named radius_action: rm authentication radiusAction radius_action

authentication-radiusPolicy

The following operations can be performed on "authentication-radiusPolicy":

unset| add| show| set| rm|

unset authentication radiusPolicy

Use this command to remove authentication radiusPolicy settings.Refer to the set authentication radiusPolicy command for meanings of the arguments.

Synopsis

unset authentication radiusPolicy <name>

add authentication radiusPolicy

Adds a RADIUS authentication policy. The policy defines the criteria under which the Citrix ADC attempts to authenticate the user with the RADIUS server.

Synopsis

add authentication radiusPolicy <name> <rule>

Arguments

name Name for the RADIUS authentication policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after RADIUS policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the RADIUS server.

reqAction Name of the RADIUS action to perform if the policy matches.

Example

To Add a Radius Policy with rule configured as ns_true and action pointing to existing radius action named radius_action: add authentication radiuspolicy radius_policy ns_true radius_action

show authentication radiusPolicy

Displays the current settings for the specified RADIUS authentication policy. If no policy name is provided, displays a list of all RADIUS authentication policies currently configured on the Citrix ADC.

Synopsis

show authentication radiusPolicy

Arguments

name Name of the RADIUS authentication policy.

Output

rule The new rule associated with the policy.

reqAction The new RADIUS action associated with the policy.

boundTo The entity name to which policy is bound

activePolicy priority bindPolicyType policyType devno count stateflag

Example

show authentication radiuspolicy radius_policy

set authentication radiusPolicy

Configures the specified RADIUS authentication policy.

Synopsis

set authentication radiusPolicy <name>

Arguments

name Name of the RADIUS authentication policy.

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the RADIUS server.

reqAction Name of the RADIUS action to perform if the policy matches.

Example

To Set a Radius Policy with a different rule and different radius action: set authentication radiuspolicy radius_policy -rule 'req.http.url contains "testradius"' -reqAction radius_action

rm authentication radiusPolicy

Removes a RADIUS authentication policy.

Synopsis

rm authentication radiusPolicy <name>

Arguments

name Name of the RADIUS authentication policy to remove.

Example

To remove a Radius Policy named radius_policy: rm authentication radiuspolicy radius_policy

authentication-samlAction

The following operations can be performed on "authentication-samlAction":

unset| show| add| rm| set|

unset authentication samlAction

Use this command to remove authentication samlAction settings.Refer to the set authentication samlAction command for meanings of the arguments.

Synopsis

unset authentication samlAction <name>

show authentication samlAction

Displays the current configuration settings for the specified SAML server profile (action).

Synopsis

show authentication samlAction

Arguments

name Name of the SAML server profile.

Output

metadataUrl This URL is used for obtaining saml metadata. Note that it fills samlIdPCertName and samlredirectUrl fields so those fields should not be updated when metadataUrl present

samlIdPCertName Name of the SSL certificate used to verify responses from SAML Identity Provider (IdP). Note that if metadateURL is present then this filed should be empty.

samlSigningCertName Name of the SSL certificate to sign requests from ServiceProvider (SP) to Identity Provider (IdP).

samlRedirectUrl URL to which users are redirected for authentication. Note that if metadateURL is present then this filed should be empty

samlACSIndex Index/ID of the metadata entry corresponding to this configuration.

samlUserField SAML user ID, as given in the SAML assertion.

samlRejectUnsignedAssertion Reject unsigned SAML assertions. ON option results in rejection of Assertion that is received without signature. STRICT option ensures that both Response and Assertion are signed. OFF allows unsigned Assertions.

samlIssuerName The name to be used in requests sent fromCitrix ADC to IdP to uniquely identify Citrix ADC.

samlTwoFactor Option to enable second factor after SAML

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

Attribute1 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute1. Maximum length of the extracted attribute is 239 bytes.

Attribute2 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute2. Maximum length of the extracted attribute is 239 bytes.

Attribute3 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute3. Maximum length of the extracted attribute is 239 bytes.

Attribute4 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute4. Maximum length of the extracted attribute is 239 bytes.

Attribute5 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute5. Maximum length of the extracted attribute is 239 bytes.

Attribute6 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute6. Maximum length of the extracted attribute is 239 bytes.

Attribute7 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute7. Maximum length of the extracted attribute is 239 bytes.

Attribute8 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute8. Maximum length of the extracted attribute is 239 bytes.

Attribute9 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute9. Maximum length of the extracted attribute is 239 bytes.

Attribute10 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute10. Maximum length of the extracted attribute is 239 bytes.

Attribute11 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute11. Maximum length of the extracted attribute is 239 bytes.

Attribute12 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute12. Maximum length of the extracted attribute is 239 bytes.

Attribute13 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute13. Maximum length of the extracted attribute is 239 bytes.

Attribute14 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute14. Maximum length of the extracted attribute is 239 bytes.

Attribute15 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute15. Maximum length of the extracted attribute is 239 bytes.

Attribute16 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute16. Maximum length of the extracted attribute is 239 bytes.

Attributes List of attribute names separated by ',' which needs to be extracted. Note that preceeding and trailing spaces will be removed. Attribute name can be 127 bytes and total length of this string should not cross 2047 bytes. These attributes have multi-value support separated by ',' and stored as key-value pair in AAA session

relaystateRule Boolean expression that will be evaluated to validate the SAML Response. Examples: set authentication samlaction <actionname> -relaystateRule 'AAA.LOGIN.RELAYSTATE.EQ("https://fqdn.com.html")' set authentication samlaction <actionname> -relaystateRule 'AAA.LOGIN.RELAYSTATE.CONTAINS("https://fqdn.com.html")' set authentication samlaction <actionname> -relaystateRule 'AAA.LOGIN.RELAYSTATE.CONTAINS_ANY("patset_name")' set authentication samlAction samlsp -relaystateRule 'AAA.LOGIN.RELAYSTATE.REGEX_MATCH(re#http://<regex>.com/#)'.

signatureAlg Algorithm to be used to sign/verify SAML transactions

digestMethod Algorithm to be used to compute/verify digest for SAML transactions

requestedAuthnContext This element specifies the authentication context requirements of authentication statements returned in the response.

authnCtxClassRef This element specifies the authentication class types that are requested from IdP (IdentityProvider). InternetProtocol: This is applicable when a principal is authenticated through the use of a provided IP address. InternetProtocolPassword: This is applicable when a principal is authenticated through the use of a provided IP address, in addition to a username/password.

Kerberos: This is applicable when the principal has authenticated using a password to a local authentication authority, in order to acquire a Kerberos ticket. MobileOneFactorUnregistered: This indicates authentication of the mobile device without requiring explicit end-user interaction. MobileTwoFactorUnregistered: This indicates two-factor based authentication during mobile customer registration process, such as secure device and user PIN. MobileOneFactorContract: Reflects mobile contract customer registration procedures and a single factor authentication. MobileTwoFactorContract: Reflects mobile contract customer registration procedures and a two-factor based authentication. Password: This class is applicable when a principal authenticates using password over unprotected http session. PasswordProtectedTransport: This class is applicable when a principal authenticates to an authentication authority through the presentation of a password over a protected session. PreviousSession: This class is applicable when a principal had authenticated to an authentication authority at some point in the past using any authentication context. X509: This indicates that the principal authenticated by means of a digital signature where the key was validated as part of an X.509 Public Key Infrastructure. PGP: This indicates that the principal authenticated by means of a digital signature where the key was validated as part of a PGP Public Key Infrastructure. SPKI: This indicates that the principal authenticated by means of a digital signature where the key was validated via an SPKI Infrastructure. XMLDSig: This indicates that the principal authenticated by means of a digital signature according to the processing rules specified in the XML Digital Signature specification. Smartcard: This indicates that the principal has authenticated using smartcard. SmartcardPKI: This class is applicable when a principal authenticates to an authentication authority through a two-factor authentication mechanism using a smartcard with enclosed private key and a PIN. SoftwarePKI: This class is applicable when a principal uses an X.509 certificate stored in software to authenticate to the authentication authority. Telephony: This class is used to indicate that the principal authenticated via the provision of a fixed-line telephone number, transported via a telephony protocol such as ADSL. NomadTelephony: Indicates that the principal is "roaming" and authenticates via the means of the line number, a user suffix, and a password element. PersonalTelephony: This class is used to indicate that the principal authenticated via the provision of a fixed-line telephone. AuthenticatedTelephony: Indicates that the principal authenticated via the means of the line number, a user suffix, and a password element. SecureRemotePassword: This class is applicable when the authentication was performed by means of Secure Remote Password. TLSClient: This class indicates that the principal authenticated by means of a client certificate, secured with the SSL/TLS transport. TimeSyncToken: This is applicable when a principal authenticates through a time synchronization token. Unspecified: This indicates that the authentication was performed by unspecified means. Windows: This indicates that Windows integrated authentication is utilized for authentication.

customAuthnCtxClassRef This element specifies the custom authentication class reference to be sent as a part of the Authentication Request that is sent by the SP to SAML IDP. The input string must be the body of the authentication class being requested. Input format: Alphanumeric string or URL specifying the body of the Request.If more than one string has to be provided, then the same can be done by specifying the classes as a string of comma separated values. Example input: set authentication samlaction samlact1 -customAuthnCtxClassRef http://www.class1.com/LoA1,http://www.class2.com/LoA2

samlBinding This element specifies the transport mechanism of saml messages.

attributeConsumingServiceIndex Index/ID of the attribute specification at Identity Provider (IdP). IdP will locate attributes requested by SP using this index and send those attributes in Assertion

sendThumbprint Option to send thumbprint instead of x509 certificate in SAML request

enforceUserName Option to choose whether the username that is extracted from SAML assertion can be edited in login page while doing second factor

logoutURL SingleLogout URL on IdP to which logoutRequest will be sent on Citrix ADC session cleanup.

artifactResolutionServiceURL URL of the Artifact Resolution Service on IdP to which Citrix ADC will post artifact to get actual SAML token.

skewTime This option specifies the allowed clock skew in number of minutes that Citrix ADC ServiceProvider allows on an incoming assertion. For example, if skewTime is 10, then assertion would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all.

logoutBinding This element specifies the transport mechanism of saml logout messages.

forceAuthn Option that forces authentication at the Identity Provider (IdP) that receives Citrix ADC's request

groupNameField Name of the tag in assertion that contains user groups.

audience Audience for which assertion sent by IdP is applicable. This is typically entity name or url that represents ServiceProvider

metadataRefreshInterval Interval in minutes for fetching metadata from specified metadata URL

metadataImportStatus Describes metadata import status.

storeSAMLResponse Option to store entire SAML Response through the life of user session.

stateChecks Boolean expression that will be evaluated to validate HTTP requests on SAML endpoints. Examples: set authentication samlaction <actionname> -stateChecks 'HTTP.REQ.HOSTNAME.EQ("https://fqdn.com.html")'

devno count stateflag

add authentication samlAction

Creates an action (profile) for a Security Assertion Markup Language (SAML) server. The profile contains all configuration data necessary to communicate with that SAML server.

Synopsis

add authentication samlAction <name> ((-metadataUrl <string>) | {-samlIdPCertName <string>} | {-samlRedirectUrl <string>}) {-samlSigningCertName <string>} {-samlACSIndex <positive_integer>} {-samlUserField <string>} {-samlRejectUnsignedAssertion <samlRejectUnsignedAssertion>} {-samlIssuerName <string>} {-samlTwoFactor (ON | OFF)} {-signatureAlg (RSA-SHA1 | RSA-SHA256)} {-digestMethod (SHA1 | SHA256)}

Arguments

name Name for the SAML server profile (action). Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after SAML profile is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication action" or 'my authentication action').

metadataUrl This URL is used for obtaining saml metadata. Note that it fills samlIdPCertName and samlredirectUrl fields so those fields should not be updated when metadataUrl present

samlIdPCertName Name of the SSL certificate used to verify responses from SAML Identity Provider (IdP). Note that if metadateURL is present then this filed should be empty.

samlSigningCertName Name of the SSL certificate to sign requests from ServiceProvider (SP) to Identity Provider (IdP).

samlRedirectUrl URL to which users are redirected for authentication. Note that if metadateURL is present then this filed should be empty

samlACSIndex Index/ID of the metadata entry corresponding to this configuration. Default value: 255 Minimum value: 0 Maximum value: 255

samlUserField SAML user ID, as given in the SAML assertion.

samlRejectUnsignedAssertion Reject unsigned SAML assertions. ON option results in rejection of Assertion that is received without signature. STRICT option ensures that both Response and Assertion are signed. OFF allows unsigned Assertions.

Possible values: ON, OFF, STRICT Default value: ON

samlIssuerName The name to be used in requests sent fromCitrix ADC to IdP to uniquely identify Citrix ADC.

samlTwoFactor Option to enable second factor after SAML

Possible values: ON, OFF Default value: OFF

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

Attribute1 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute1. Maximum length of the extracted attribute is 239 bytes.

Attribute2 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute2. Maximum length of the extracted attribute is 239 bytes.

Attribute3 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute3. Maximum length of the extracted attribute is 239 bytes.

Attribute4 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute4. Maximum length of the extracted attribute is 239 bytes.

Attribute5 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute5. Maximum length of the extracted attribute is 239 bytes.

Attribute6 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute6. Maximum length of the extracted attribute is 239 bytes.

Attribute7 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute7. Maximum length of the extracted attribute is 239 bytes.

Attribute8 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute8. Maximum length of the extracted attribute is 239 bytes.

Attribute9 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute9. Maximum length of the extracted attribute is 239 bytes.

Attribute10 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute10. Maximum length of the extracted attribute is 239 bytes.

Attribute11 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute11. Maximum length of the extracted attribute is 239 bytes.

Attribute12 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute12. Maximum length of the extracted attribute is 239 bytes.

Attribute13 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute13. Maximum length of the extracted attribute is 239 bytes.

Attribute14 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute14. Maximum length of the extracted attribute is 239 bytes.

Attribute15 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute15. Maximum length of the extracted attribute is 239 bytes.

Attribute16 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute16. Maximum length of the extracted attribute is 239 bytes.

Attributes List of attribute names separated by ',' which needs to be extracted. Note that preceeding and trailing spaces will be removed. Attribute name can be 127 bytes and total length of this string should not cross 2047 bytes. These attributes have multi-value support separated by ',' and stored as key-value pair in AAA session

relaystateRule Boolean expression that will be evaluated to validate the SAML Response. Examples: set authentication samlaction <actionname> -relaystateRule 'AAA.LOGIN.RELAYSTATE.EQ("https://fqdn.com.html")' set authentication samlaction <actionname> -relaystateRule 'AAA.LOGIN.RELAYSTATE.CONTAINS("https://fqdn.com.html")' set authentication samlaction <actionname> -relaystateRule 'AAA.LOGIN.RELAYSTATE.CONTAINS_ANY("patset_name")' set authentication samlAction samlsp -relaystateRule 'AAA.LOGIN.RELAYSTATE.REGEX_MATCH(re#http://<regex>.com/#)'.

signatureAlg Algorithm to be used to sign/verify SAML transactions

Possible values: RSA-SHA1, RSA-SHA256 Default value: RSA-SHA256

digestMethod Algorithm to be used to compute/verify digest for SAML transactions

Possible values: SHA1, SHA256 Default value: SHA256

requestedAuthnContext This element specifies the authentication context requirements of authentication statements returned in the response.

Possible values: exact, minimum, maximum, better Default value: exact

authnCtxClassRef This element specifies the authentication class types that are requested from IdP (IdentityProvider). InternetProtocol: This is applicable when a principal is authenticated through the use of a provided IP address. InternetProtocolPassword: This is applicable when a principal is authenticated through the use of a provided IP address, in addition to a username/password. Kerberos: This is applicable when the principal has authenticated using a password to a local authentication authority, in order to acquire a Kerberos ticket. MobileOneFactorUnregistered: This indicates authentication of the mobile device without requiring explicit end-user interaction. MobileTwoFactorUnregistered: This indicates two-factor based authentication during mobile customer registration process, such as secure device and user PIN. MobileOneFactorContract: Reflects mobile contract customer registration procedures and a single factor authentication. MobileTwoFactorContract: Reflects mobile contract customer registration procedures and a two-factor based authentication. Password: This class is applicable when a principal authenticates using password over unprotected http session. PasswordProtectedTransport: This class is applicable when a principal authenticates to an authentication authority through the presentation of a password over a protected session. PreviousSession: This class is applicable when a principal had authenticated to an authentication authority at some point in the past using any authentication context. X509: This indicates that the principal authenticated by means of a digital signature where the key was validated as part of an X.509 Public Key Infrastructure. PGP: This indicates that the principal authenticated by means of a digital signature where the key was validated as part of a PGP Public Key Infrastructure. SPKI: This indicates that the principal authenticated by means of a digital signature where the key was validated via an SPKI Infrastructure. XMLDSig: This indicates that the principal authenticated by means of a digital signature according to the processing rules specified in the XML Digital Signature specification. Smartcard: This indicates that the principal has authenticated using smartcard. SmartcardPKI: This class is applicable when a principal authenticates to an authentication authority through a two-factor authentication mechanism using a smartcard with enclosed private key and a PIN. SoftwarePKI: This class is applicable when a principal uses an X.509 certificate stored in software to authenticate to the authentication authority. Telephony: This class is used to indicate that the principal authenticated via the provision of a fixed-line telephone number, transported via a telephony protocol such as ADSL. NomadTelephony: Indicates that the principal is "roaming" and authenticates via the means of the line number, a user suffix, and a password element. PersonalTelephony: This class is used to indicate that the principal authenticated via the provision of a fixed-line telephone.

AuthenticatedTelephony: Indicates that the principal authenticated via the means of the line number, a user suffix, and a password element. SecureRemotePassword: This class is applicable when the authentication was performed by means of Secure Remote Password. TLSClient: This class indicates that the principal authenticated by means of a client certificate, secured with the SSL/TLS transport. TimeSyncToken: This is applicable when a principal authenticates through a time synchronization token. Unspecified: This indicates that the authentication was performed by unspecified means. Windows: This indicates that Windows integrated authentication is utilized for authentication.

customAuthnCtxClassRef This element specifies the custom authentication class reference to be sent as a part of the Authentication Request that is sent by the SP to SAML IDP. The input string must be the body of the authentication class being requested. Input format: Alphanumeric string or URL specifying the body of the Request.If more than one string has to be provided, then the same can be done by specifying the classes as a string of comma separated values. Example input: set authentication samlaction samlact1 -customAuthnCtxClassRef http://www.class1.com/LoA1,http://www.class2.com/LoA2

samlBinding This element specifies the transport mechanism of saml messages.

Possible values: REDIRECT, POST, ARTIFACT Default value: POST

attributeConsumingServiceIndex Index/ID of the attribute specification at Identity Provider (IdP). IdP will locate attributes requested by SP using this index and send those attributes in Assertion Default value: 255 Minimum value: 0 Maximum value: 255

sendThumbprint Option to send thumbprint instead of x509 certificate in SAML request

Possible values: ON, OFF Default value: OFF

enforceUserName Option to choose whether the username that is extracted from SAML assertion can be edited in login page while doing second factor

Possible values: ON, OFF Default value: ON

logoutURL SingleLogout URL on IdP to which logoutRequest will be sent on Citrix ADC session cleanup.

artifactResolutionServiceURL URL of the Artifact Resolution Service on IdP to which Citrix ADC will post artifact to get actual SAML token.

skewTime This option specifies the allowed clock skew in number of minutes that Citrix ADC ServiceProvider allows on an incoming assertion. For example, if skewTime is 10, then assertion would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all. Default value: 5

logoutBinding This element specifies the transport mechanism of saml logout messages.

Possible values: REDIRECT, POST Default value: POST

forceAuthn Option that forces authentication at the Identity Provider (IdP) that receives Citrix ADC's request

Possible values: ON, OFF Default value: OFF

groupNameField Name of the tag in assertion that contains user groups.

audience Audience for which assertion sent by IdP is applicable. This is typically entity name or url that represents ServiceProvider

metadataRefreshInterval Interval in minutes for fetching metadata from specified metadata URL Default value: 3600 Minimum value: 0

storeSAMLResponse Option to store entire SAML Response through the life of user session.

Possible values: ON, OFF Default value: OFF

stateChecks Boolean expression that will be evaluated to validate HTTP requests on SAML endpoints. Examples: set authentication samlaction <actionname> -stateChecks 'HTTP.REQ.HOSTNAME.EQ("https://fqdn.com.html")'

rm authentication samlAction

Removes a SAML profile (action). An action cannot be removed if it is bound to a policy.

Synopsis

rm authentication samlAction <name>

Arguments

name Name of the SAML profile to be removed.

set authentication samlAction

Modifies the specified parameters of a SAML server profile (action).

Synopsis

set authentication samlAction <name>

Arguments

name Name of the SAML profile (action) to modify.

metadataUrl This URL is used for obtaining saml metadata. Note that it fills samlIdPCertName and samlredirectUrl fields so those fields should not be updated when metadataUrl present

samlIdPCertName Name of the SSL certificate used to verify responses from SAML Identity Provider (IdP). Note that if metadateURL is present then this filed should be empty.

samlSigningCertName Name of the SSL certificate to sign requests from ServiceProvider (SP) to Identity Provider (IdP).

samlRedirectUrl URL to which users are redirected for authentication. Note that if metadateURL is present then this filed should be empty

samlACSIndex Index/ID of the metadata entry corresponding to this configuration. Default value: 255 Minimum value: 0 Maximum value: 255

samlUserField SAML user ID, as given in the SAML assertion.

samlRejectUnsignedAssertion Reject unsigned SAML assertions. ON option results in rejection of Assertion that is received without signature. STRICT option ensures that both Response and Assertion are signed. OFF allows unsigned Assertions.

Possible values: ON, OFF, STRICT Default value: ON

samlIssuerName The name to be used in requests sent fromCitrix ADC to IdP to uniquely identify Citrix ADC.

samlTwoFactor Option to enable second factor after SAML

Possible values: ON, OFF Default value: OFF

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

Attribute1 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute1. Maximum length of the extracted attribute is 239 bytes.

Attribute2 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute2. Maximum length of the extracted attribute is 239 bytes.

Attribute3 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute3. Maximum length of the extracted attribute is 239 bytes.

Attribute4 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute4. Maximum length of the extracted attribute is 239 bytes.

Attribute5 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute5. Maximum length of the extracted attribute is 239 bytes.

Attribute6 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute6. Maximum length of the extracted attribute is 239 bytes.

Attribute7 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute7. Maximum length of the extracted attribute is 239 bytes.

Attribute8 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute8. Maximum length of the extracted attribute is 239 bytes.

Attribute9 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute9. Maximum length of the extracted attribute is 239 bytes.

Attribute10 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute10. Maximum length of the extracted attribute is 239 bytes.

Attribute11 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute11. Maximum length of the extracted attribute is 239 bytes.

Attribute12 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute12. Maximum length of the extracted attribute is 239 bytes.

Attribute13 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute13. Maximum length of the extracted attribute is 239 bytes.

Attribute14 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute14. Maximum length of the extracted attribute is 239 bytes.

Attribute15 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute15. Maximum length of the extracted attribute is 239 bytes.

Attribute16 Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute16. Maximum length of the extracted attribute is 239 bytes.

Attributes List of attribute names separated by ',' which needs to be extracted. Note that preceeding and trailing spaces will be removed. Attribute name can be 127 bytes and total length of this string should not cross 2047 bytes. These attributes have multi-value support separated by ',' and stored as key-value pair in AAA session

relaystateRule Boolean expression that will be evaluated to validate the SAML Response. Examples: set authentication samlaction <actionname> -relaystateRule 'AAA.LOGIN.RELAYSTATE.EQ("https://fqdn.com.html")' set authentication samlaction <actionname> -relaystateRule 'AAA.LOGIN.RELAYSTATE.CONTAINS("https://fqdn.com.html")' set authentication samlaction <actionname> -relaystateRule 'AAA.LOGIN.RELAYSTATE.CONTAINS_ANY("patset_name")' set authentication samlAction samlsp -relaystateRule 'AAA.LOGIN.RELAYSTATE.REGEX_MATCH(re#http://<regex>.com/#)'.

signatureAlg Algorithm to be used to sign/verify SAML transactions

Possible values: RSA-SHA1, RSA-SHA256 Default value: RSA-SHA256

digestMethod Algorithm to be used to compute/verify digest for SAML transactions

Possible values: SHA1, SHA256 Default value: SHA256

requestedAuthnContext This element specifies the authentication context requirements of authentication statements returned in the response.

Possible values: exact, minimum, maximum, better Default value: exact

authnCtxClassRef This element specifies the authentication class types that are requested from IdP (IdentityProvider). InternetProtocol: This is applicable when a principal is authenticated through the use of a provided IP address. InternetProtocolPassword: This is applicable when a principal is authenticated through the use of a provided IP address, in addition to a username/password. Kerberos: This is applicable when the principal has authenticated using a password to a local authentication authority, in order to acquire a Kerberos ticket. MobileOneFactorUnregistered: This indicates authentication of the mobile device without requiring explicit end-user interaction. MobileTwoFactorUnregistered: This indicates two-factor based authentication during mobile customer registration process, such as secure device and user PIN. MobileOneFactorContract: Reflects mobile contract customer registration procedures and a single factor authentication. MobileTwoFactorContract: Reflects mobile contract customer registration procedures and a two-factor based authentication. Password: This class is applicable when a principal authenticates

using password over unprotected http session. PasswordProtectedTransport: This class is applicable when a principal authenticates to an authentication authority through the presentation of a password over a protected session. PreviousSession: This class is applicable when a principal had authenticated to an authentication authority at some point in the past using any authentication context. X509: This indicates that the principal authenticated by means of a digital signature where the key was validated as part of an X.509 Public Key Infrastructure. PGP: This indicates that the principal authenticated by means of a digital signature where the key was validated as part of a PGP Public Key Infrastructure. SPKI: This indicates that the principal authenticated by means of a digital signature where the key was validated via an SPKI Infrastructure. XMLDSig: This indicates that the principal authenticated by means of a digital signature according to the processing rules specified in the XML Digital Signature specification. Smartcard: This indicates that the principal has authenticated using smartcard. SmartcardPKI: This class is applicable when a principal authenticates to an authentication authority through a two-factor authentication mechanism using a smartcard with enclosed private key and a PIN. SoftwarePKI: This class is applicable when a principal uses an X.509 certificate stored in software to authenticate to the authentication authority. Telephony: This class is used to indicate that the principal authenticated via the provision of a fixed-line telephone number, transported via a telephony protocol such as ADSL. NomadTelephony: Indicates that the principal is "roaming" and authenticates via the means of the line number, a user suffix, and a password element. PersonalTelephony: This class is used to indicate that the principal authenticated via the provision of a fixed-line telephone. AuthenticatedTelephony: Indicates that the principal authenticated via the means of the line number, a user suffix, and a password element. SecureRemotePassword: This class is applicable when the authentication was performed by means of Secure Remote Password. TLSClient: This class indicates that the principal authenticated by means of a client certificate, secured with the SSL/TLS transport. TimeSyncToken: This is applicable when a principal authenticates through a time synchronization token. Unspecified: This indicates that the authentication was performed by unspecified means. Windows: This indicates that Windows integrated authentication is utilized for authentication.

customAuthnCtxClassRef This element specifies the custom authentication class reference to be sent as a part of the Authentication Request that is sent by the SP to SAML IDP. The input string must be the body of the authentication class being requested. Input format: Alphanumeric string or URL specifying the body of the Request.If more than one string has to be provided, then the same can be done by specifying the classes as a string of comma separated values. Example input: set authentication samlaction samlact1 -customAuthnCtxClassRef http://www.class1.com/LoA1,http://www.class2.com/LoA2

samlBinding This element specifies the transport mechanism of saml messages.

Possible values: REDIRECT, POST, ARTIFACT Default value: POST

attributeConsumingServiceIndex Index/ID of the attribute specification at Identity Provider (IdP). IdP will locate attributes requested by SP using this index and send those attributes in Assertion Default value: 255 Minimum value: 0 Maximum value: 255

sendThumbprint Option to send thumbprint instead of x509 certificate in SAML request

Possible values: ON, OFF Default value: OFF

enforceUserName Option to choose whether the username that is extracted from SAML assertion can be edited in login page while doing second factor

Possible values: ON, OFF Default value: ON

logoutURL SingleLogout URL on IdP to which logoutRequest will be sent on Citrix ADC session cleanup.

artifactResolutionServiceURL URL of the Artifact Resolution Service on IdP to which Citrix ADC will post artifact to get actual SAML token.

skewTime This option specifies the allowed clock skew in number of minutes that Citrix ADC ServiceProvider allows on an incoming assertion. For example, if skewTime is 10, then assertion would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all. Default value: 5

logoutBinding This element specifies the transport mechanism of saml logout messages.

Possible values: REDIRECT, POST Default value: POST

forceAuthn Option that forces authentication at the Identity Provider (IdP) that receives Citrix ADC's request

Possible values: ON, OFF Default value: OFF

groupNameField Name of the tag in assertion that contains user groups.

audience Audience for which assertion sent by IdP is applicable. This is typically entity name or url that represents ServiceProvider

metadataRefreshInterval Interval in minutes for fetching metadata from specified metadata URL Default value: 3600 Minimum value: 0

storeSAMLResponse Option to store entire SAML Response through the life of user session.

Possible values: ON, OFF Default value: OFF

stateChecks Boolean expression that will be evaluated to validate HTTP requests on SAML endpoints. Examples: set authentication samlaction <actionname> -stateChecks 'HTTP.REQ.HOSTNAME.EQ("https://fqdn.com.html")'

authentication-samlIdPPolicy

The following operations can be performed on "authentication-samlIdPPolicy":

rm| stat| show| unset| rename| set| add|

rm authentication samlIdPPolicy

Removes an existing SAML Identity Provider (IdP) policy.

Synopsis

rm authentication samlIdPPolicy <name>

Arguments

name Name of the authentication policy to remove.

stat authentication samlIdPPolicy

Display SAML Identity Provider (IdP) policy statistics.

Synopsis

stat authentication samlIdPPolicy

Arguments

name The name of the SAML Identity Provider (IdP) policy for which statistics will be displayed. If not given statistics are shown for all policies.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Example

stat authentication samlidppolicy.

Related Commands

- stat authentication OAuthIdPPolicy

show authentication samlIdPPolicy

Displays information about all configured SAML Identity Provider (IdP) authentication policies, or displays detailed information about the specified policy.

Synopsis

show authentication samlIdPPolicy

Arguments

name Name of the SAML IdentityProvider (IdP) policy for which to display detailed information.

Output

rule The rule used by the SAML Identity Provider (IdP) authentication policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide

action The action to be performed when the rule is matched.

stateflag undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

comment Any comments to preserve information about this policy.

logAction Name of messagelog action to use when a request matches this policy.

boundTo The entity name to which policy is bound

activePolicy priority gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

hits Number of hits.

bindPolicyType vserverType devno count

unset authentication samlIdPPolicy

Removes the settings of an existing SAML IdentityProvider (IdP) policy. Attributes for which a default value is available revert to their default values. See the set samlIdPPolicy command for a description of the parameters..Refer to the set authentication samlIdPPolicy command for meanings of the arguments.

Synopsis

unset authentication samlIdPPolicy <name>

Example

unset samlIdpPolicy pol9 -undefAction

rename authentication samlIdPPolicy

Renames the specified SAML IdentityProvider (IdP) policy. You must restart the Citrix ADC to put new name in effect.

Synopsis

rename authentication samlIdPPolicy <name>@ <newName>@

Arguments

name Existing name of the SAML IdentityProvider policy.

newName New name for the SAML IdentityProvider policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my samlidppolicy policy" or 'my samlidppolicy policy').

Example

rename samlidppolicy policy oldname newname

set authentication samlIdPPolicy

Modifies the specified parameters of an existing SAML IdentityProvider (IdP) policy.

Synopsis

set authentication samlIdPPolicy <name>

Arguments

name Name of the SAML Identity Provider (IdP) authentication policy to modify.

rule Expression which is evaluated to choose a profile for authentication.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the profile to apply to requests or connections that match this policy.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

comment Any comments to preserve information about this policy.

logAction Name of messagelog action to use when a request matches this policy.

add authentication samlIdPPolicy

Adds a SAML Identity Provider (IdP) policy to use for use in authentication.

Synopsis

add authentication samlIdPPolicy <name> -rule <expression> -action <string>

Arguments

name Name for the SAML Identity Provider (IdP) authentication policy. This is used for configuring Citrix ADC as SAML Identity Provider. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

rule Expression which is evaluated to choose a profile for authentication.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the profile to apply to requests or connections that match this policy.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

comment Any comments to preserve information about this policy.

logAction Name of messagelog action to use when a request matches this policy.

authentication-samlIdPProfile

The following operations can be performed on "authentication-samlIdPProfile":

set| show| rm| unset| add|

set authentication samlIdPProfile

Modifies the specified attributes of a saml IdP profile.

Synopsis

set authentication samlIdPProfile <name> [-Attribute1 <string> -Attribute1Expr <string>] [-Attribute2 <string> -Attribute2Expr <string>] [-Attribute3 <string> -Attribute3Expr <string>] [-Attribute4 <string> -Attribute4Expr <string>] [-Attribute5 <string> -Attribute5Expr <string>] [-Attribute6 <string> -Attribute6Expr <string>] [-Attribute7 <string> -Attribute7Expr <string>] [-Attribute8 <string> -Attribute8Expr <string>] [-Attribute9 <string> -Attribute9Expr <string>] [-Attribute10 <string> -Attribute10Expr <string>] [-Attribute11 <string> -Attribute11Expr <string>] [-Attribute12 <string> -Attribute12Expr <string>] [-Attribute13 <string> -Attribute13Expr <string>] [-Attribute14 <string> -Attribute14Expr <string>] [-Attribute15 <string> -Attribute15Expr <string>] [-Attribute16 <string> -Attribute16Expr <string>]

Arguments

name Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

samlSPCertName Name of the SSL certificate of SAML Relying Party. This certificate is used to verify signature of the incoming AuthnRequest from a Relying Party or Service Provider

samlIdPCertName Name of the certificate used to sign the SAMLResposne that is sent to Relying Party or Service Provider after successful authentication

assertionConsumerServiceURL URL to which the assertion is to be sent.

samlIssuerName The name to be used in requests sent fromCitrix ADC to IdP to uniquely identify Citrix ADC.

rejectUnsignedRequests Option to Reject unsigned SAML Requests. ON option denies any authentication requests that arrive without signature.

Possible values: ON, OFF Default value: ON

signatureAlg Algorithm to be used to sign/verify SAML transactions

Possible values: RSA-SHA1, RSA-SHA256 Default value: RSA-SHA256

digestMethod Algorithm to be used to compute/verify digest for SAML transactions

Possible values: SHA1, SHA256 Default value: SHA256

audience Audience for which assertion sent by IdP is applicable. This is typically entity name or url that represents ServiceProvider

NameIDFormat Format of Name Identifier sent in Assertion.

Possible values: Unspecified, emailAddress, X509SubjectName, WindowsDomainQualifiedName, kerberos, entity, persistent, transient Default value: transient

NameIDExpr Expression that will be evaluated to obtain NameIdentifier to be sent in assertion

Attribute1 Name of attribute1 that needs to be sent in SAML Assertion

Attribute1Expr Expression that will be evaluated to obtain attribute1's value to be sent in Assertion

Attribute1FriendlyName User-Friendly Name of attribute1 that needs to be sent in SAML Assertion

Attribute1Format Format of Attribute1 to be sent in Assertion.

Possible values: URI, Basic

Attribute2 Name of attribute2 that needs to be sent in SAML Assertion

Attribute2Expr Expression that will be evaluated to obtain attribute2's value to be sent in Assertion

Attribute2FriendlyName User-Friendly Name of attribute2 that needs to be sent in SAML Assertion

Attribute2Format Format of Attribute2 to be sent in Assertion.

Possible values: URI, Basic

Attribute3 Name of attribute3 that needs to be sent in SAML Assertion

Attribute3Expr Expression that will be evaluated to obtain attribute3's value to be sent in Assertion

Attribute3FriendlyName User-Friendly Name of attribute3 that needs to be sent in SAML Assertion

Attribute3Format Format of Attribute3 to be sent in Assertion.

Possible values: URI, Basic

Attribute4 Name of attribute4 that needs to be sent in SAML Assertion

Attribute4Expr Expression that will be evaluated to obtain attribute4's value to be sent in Assertion

Attribute4FriendlyName User-Friendly Name of attribute4 that needs to be sent in SAML Assertion

Attribute4Format Format of Attribute4 to be sent in Assertion.

Possible values: URI, Basic

Attribute5 Name of attribute5 that needs to be sent in SAML Assertion

Attribute5Expr Expression that will be evaluated to obtain attribute5's value to be sent in Assertion

Attribute5FriendlyName User-Friendly Name of attribute5 that needs to be sent in SAML Assertion

Attribute5Format Format of Attribute5 to be sent in Assertion.

Possible values: URI, Basic

Attribute6 Name of attribute6 that needs to be sent in SAML Assertion

Attribute6Expr Expression that will be evaluated to obtain attribute6's value to be sent in Assertion

Attribute6FriendlyName User-Friendly Name of attribute6 that needs to be sent in SAML Assertion

Attribute6Format Format of Attribute6 to be sent in Assertion.

Possible values: URI, Basic

Attribute7 Name of attribute7 that needs to be sent in SAML Assertion

Attribute7Expr Expression that will be evaluated to obtain attribute7's value to be sent in Assertion

Attribute7FriendlyName User-Friendly Name of attribute7 that needs to be sent in SAML Assertion

Attribute7Format Format of Attribute7 to be sent in Assertion.

Possible values: URI, Basic

Attribute8 Name of attribute8 that needs to be sent in SAML Assertion

Attribute8Expr Expression that will be evaluated to obtain attribute8's value to be sent in Assertion

Attribute8FriendlyName User-Friendly Name of attribute8 that needs to be sent in SAML Assertion

Attribute8Format Format of Attribute8 to be sent in Assertion.

Possible values: URI, Basic

Attribute9 Name of attribute9 that needs to be sent in SAML Assertion

Attribute9Expr Expression that will be evaluated to obtain attribute9's value to be sent in Assertion

Attribute9FriendlyName User-Friendly Name of attribute9 that needs to be sent in SAML Assertion

Attribute9Format Format of Attribute9 to be sent in Assertion.

Possible values: URI, Basic

Attribute10 Name of attribute10 that needs to be sent in SAML Assertion

Attribute10Expr Expression that will be evaluated to obtain attribute10's value to be sent in Assertion

Attribute10FriendlyName User-Friendly Name of attribute10 that needs to be sent in SAML Assertion

Attribute10Format Format of Attribute10 to be sent in Assertion.

Possible values: URI, Basic

Attribute11 Name of attribute11 that needs to be sent in SAML Assertion

Attribute11Expr Expression that will be evaluated to obtain attribute11's value to be sent in Assertion

Attribute11FriendlyName User-Friendly Name of attribute11 that needs to be sent in SAML Assertion

Attribute11Format Format of Attribute11 to be sent in Assertion.

Possible values: URI, Basic

Attribute12 Name of attribute12 that needs to be sent in SAML Assertion

Attribute12Expr Expression that will be evaluated to obtain attribute12's value to be sent in Assertion

Attribute12FriendlyName User-Friendly Name of attribute12 that needs to be sent in SAML Assertion

Attribute12Format Format of Attribute12 to be sent in Assertion.

Possible values: URI, Basic

Attribute13 Name of attribute13 that needs to be sent in SAML Assertion

Attribute13Expr Expression that will be evaluated to obtain attribute13's value to be sent in Assertion

Attribute13FriendlyName User-Friendly Name of attribute13 that needs to be sent in SAML Assertion

Attribute13Format Format of Attribute13 to be sent in Assertion.

Possible values: URI, Basic

Attribute14 Name of attribute14 that needs to be sent in SAML Assertion

Attribute14Expr Expression that will be evaluated to obtain attribute14's value to be sent in Assertion

Attribute14FriendlyName User-Friendly Name of attribute14 that needs to be sent in SAML Assertion

Attribute14Format Format of Attribute14 to be sent in Assertion.

Possible values: URI, Basic

Attribute15 Name of attribute15 that needs to be sent in SAML Assertion

Attribute15Expr Expression that will be evaluated to obtain attribute15's value to be sent in Assertion

Attribute15FriendlyName User-Friendly Name of attribute15 that needs to be sent in SAML Assertion

Attribute15Format Format of Attribute15 to be sent in Assertion.

Possible values: URI, Basic

Attribute16 Name of attribute16 that needs to be sent in SAML Assertion

Attribute16Expr Expression that will be evaluated to obtain attribute16's value to be sent in Assertion

Attribute16FriendlyName User-Friendly Name of attribute16 that needs to be sent in SAML Assertion

Attribute16Format Format of Attribute16 to be sent in Assertion.

Possible values: URI, Basic

encryptAssertion Option to encrypt assertion when Citrix ADC IDP sends one.

Possible values: ON, OFF Default value: OFF

encryptionAlgorithm Algorithm to be used to encrypt SAML assertion

Possible values: DES3, AES128, AES192, AES256 Default value: AES256

samlBinding This element specifies the transport mechanism of saml messages.

Possible values: REDIRECT, POST, ARTIFACT Default value: POST

skewTime This option specifies the number of minutes on either side of current time that the assertion would be valid. For example, if skewTime is 10, then assertion would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all. Default value: 5

serviceProviderID Unique identifier of the Service Provider that sends SAML Request. Citrix ADC will ensure that the Issuer of the SAML Request matches this URI. In case of SP initiated sign-in scenarios, this value must be same as samlIssuerName configured in samlAction.

signAssertion Option to sign portions of assertion when Citrix ADC IDP sends one. Based on the user selection, either Assertion or Response or Both or none can be signed

Possible values: NONE, ASSERTION, RESPONSE, BOTH Default value: ASSERTION

keyTransportAlg Key transport algorithm to be used in encryption of SAML assertion

Possible values: RSA-V1_5, RSA_OAEP Default value: RSA_OAEP

SPLogoutUrl Endpoint on the ServiceProvider (SP) to which logout messages are to be sent

logoutBinding This element specifies the transport mechanism of saml logout messages.

Possible values: REDIRECT, POST Default value: POST

defaultAuthenticationGroup This group will be part of AAA session's internal group list. This will be helpful to admin in Nfactor flow to decide right AAA configuration for Relaying Party. In authentication policy AAA.USER.IS_MEMBER_OF("<default_auth_group>") is way to use this feature.

metadataUrl This URL is used for obtaining samlidp metadata

metadataRefreshInterval Interval in minute for fetching metadata from specified metadata URL Default value: 3600 Minimum value: 0

signatureService Name of the service in cloud used to sign the data

samlSigningCertVersion version of the certificate in signature service used to sign the SAMLResposne that is sent to Relying Party or Service Provider after successful authentication

samlSPCertVersion version of the certificate in signature service used to verify the signature of the incoming AuthnRequest from a Relying Party or Service Provider

acsUrlRule Expression that will be evaluated to allow Assertion Consumer Service URI coming in the SAML Request

show authentication samlIdPProfile

Displays information about all configured saml single sign-on profiles, or displays detailed information about the specified action.

Synopsis

show authentication samlIdPProfile

Arguments

name Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

Output

samlSPCertName Name of the SSL certificate of SAML Relying Party. This certificate is used to verify signature of the incoming AuthnRequest from a Relying Party or Service Provider

samlIdPCertName Name of the certificate used to sign the SAMLResposne that is sent to Relying Party or Service Provider after successful authentication

assertionConsumerServiceURL URL to which the assertion is to be sent.

sendPassword Option to send password in assertion.

samlIssuerName The name to be used in requests sent fromCitrix ADC to IdP to uniquely identify Citrix ADC.

rejectUnsignedRequests Option to Reject unsigned SAML Requests. ON option denies any authentication requests that arrive without signature.

signatureAlg Algorithm to be used to sign/verify SAML transactions

digestMethod Algorithm to be used to compute/verify digest for SAML transactions

audience Audience for which assertion sent by IdP is applicable. This is typically entity name or url that represents ServiceProvider

NameIDFormat Format of Name Identifier sent in Assertion.

NameIDExpr Expression that will be evaluated to obtain NameIdentifier to be sent in assertion

Attribute1 Name of attribute1 that needs to be sent in SAML Assertion

Attribute2 Name of attribute2 that needs to be sent in SAML Assertion

Attribute3 Name of attribute3 that needs to be sent in SAML Assertion

Attribute4 Name of attribute4 that needs to be sent in SAML Assertion

Attribute5 Name of attribute5 that needs to be sent in SAML Assertion

Attribute6 Name of attribute6 that needs to be sent in SAML Assertion

Attribute7 Name of attribute7 that needs to be sent in SAML Assertion

Attribute8 Name of attribute8 that needs to be sent in SAML Assertion

Attribute9 Name of attribute9 that needs to be sent in SAML Assertion

Attribute10 Name of attribute10 that needs to be sent in SAML Assertion

Attribute11 Name of attribute11 that needs to be sent in SAML Assertion

Attribute12 Name of attribute12 that needs to be sent in SAML Assertion

Attribute13 Name of attribute13 that needs to be sent in SAML Assertion

Attribute14 Name of attribute14 that needs to be sent in SAML Assertion

Attribute15 Name of attribute15 that needs to be sent in SAML Assertion

Attribute16 Name of attribute16 that needs to be sent in SAML Assertion

Attribute1FriendlyName User-Friendly Name of attribute1 that needs to be sent in SAML Assertion

Attribute2FriendlyName User-Friendly Name of attribute2 that needs to be sent in SAML Assertion

Attribute3FriendlyName User-Friendly Name of attribute3 that needs to be sent in SAML Assertion

Attribute4FriendlyName User-Friendly Name of attribute4 that needs to be sent in SAML Assertion

Attribute5FriendlyName User-Friendly Name of attribute5 that needs to be sent in SAML Assertion

Attribute6FriendlyName User-Friendly Name of attribute6 that needs to be sent in SAML Assertion

Attribute7FriendlyName User-Friendly Name of attribute7 that needs to be sent in SAML Assertion

Attribute8FriendlyName User-Friendly Name of attribute8 that needs to be sent in SAML Assertion

Attribute9FriendlyName User-Friendly Name of attribute9 that needs to be sent in SAML Assertion

Attribute10FriendlyName User-Friendly Name of attribute10 that needs to be sent in SAML Assertion

Attribute11FriendlyName User-Friendly Name of attribute11 that needs to be sent in SAML Assertion

Attribute12FriendlyName User-Friendly Name of attribute12 that needs to be sent in SAML Assertion

Attribute13FriendlyName User-Friendly Name of attribute13 that needs to be sent in SAML Assertion

Attribute14FriendlyName User-Friendly Name of attribute14 that needs to be sent in SAML Assertion

Attribute15FriendlyName User-Friendly Name of attribute15 that needs to be sent in SAML Assertion

Attribute16FriendlyName User-Friendly Name of attribute16 that needs to be sent in SAML Assertion

Attribute1Format Format of Attribute1 to be sent in Assertion.

Attribute2Format Format of Attribute2 to be sent in Assertion.

Attribute3Format Format of Attribute3 to be sent in Assertion.

Attribute4Format Format of Attribute4 to be sent in Assertion.

Attribute5Format Format of Attribute5 to be sent in Assertion.

Attribute6Format Format of Attribute6 to be sent in Assertion.

Attribute7Format Format of Attribute7 to be sent in Assertion.

Attribute8Format Format of Attribute8 to be sent in Assertion.

Attribute9Format Format of Attribute9 to be sent in Assertion.

Attribute10Format Format of Attribute10 to be sent in Assertion.

Attribute11Format Format of Attribute11 to be sent in Assertion.

Attribute12Format Format of Attribute12 to be sent in Assertion.

Attribute13Format Format of Attribute13 to be sent in Assertion.

Attribute14Format Format of Attribute14 to be sent in Assertion.

Attribute15Format Format of Attribute15 to be sent in Assertion.

Attribute16Format Format of Attribute16 to be sent in Assertion.

Attribute1Expr Expression that will be evaluated to obtain attribute1's value to be sent in Assertion

Attribute2Expr Expression that will be evaluated to obtain attribute2's value to be sent in Assertion

Attribute3Expr Expression that will be evaluated to obtain attribute3's value to be sent in Assertion

Attribute4Expr Expression that will be evaluated to obtain attribute4's value to be sent in Assertion

Attribute5Expr Expression that will be evaluated to obtain attribute5's value to be sent in Assertion

Attribute6Expr Expression that will be evaluated to obtain attribute6's value to be sent in Assertion

Attribute7Expr Expression that will be evaluated to obtain attribute7's value to be sent in Assertion

Attribute8Expr Expression that will be evaluated to obtain attribute8's value to be sent in Assertion

Attribute9Expr Expression that will be evaluated to obtain attribute9's value to be sent in Assertion

Attribute10Expr Expression that will be evaluated to obtain attribute10's value to be sent in Assertion

Attribute11Expr Expression that will be evaluated to obtain attribute11's value to be sent in Assertion

Attribute12Expr Expression that will be evaluated to obtain attribute12's value to be sent in Assertion

Attribute13Expr Expression that will be evaluated to obtain attribute13's value to be sent in Assertion

Attribute14Expr Expression that will be evaluated to obtain attribute14's value to be sent in Assertion

Attribute15Expr Expression that will be evaluated to obtain attribute15's value to be sent in Assertion

Attribute16Expr Expression that will be evaluated to obtain attribute16's value to be sent in Assertion

encryptAssertion Option to encrypt assertion when Citrix ADC IDP sends one.

encryptionAlgorithm Algorithm to be used to encrypt SAML assertion

samlBinding This element specifies the transport mechanism of saml messages.

skewTime This option specifies the number of minutes on either side of current time that the assertion would be valid. For example, if skewTime is 10, then assertion would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all.

serviceProviderID Unique identifier of the Service Provider that sends SAML Request. Citrix ADC will ensure that the Issuer of the SAML Request matches this URI. In case of SP initiated sign-in scenarios, this value must be same as samlIssuerName configured in samlAction.

signAssertion Option to sign portions of assertion when Citrix ADC IDP sends one. Based on the user selection, either Assertion or Response or Both or none can be signed

keyTransportAlg Key transport algorithm to be used in encryption of SAML assertion

SPLogoutUrl Endpoint on the ServiceProvider (SP) to which logout messages are to be sent

logoutBinding This element specifies the transport mechanism of saml logout messages.

defaultAuthenticationGroup This group will be part of AAA session's internal group list. This will be helpful to admin in Nfactor flow to decide right AAA configuration for Relaying Party. In authentication policy AAA.USER.IS_MEMBER_OF("<default_auth_group>") is way to use this feature.

metadataUrl This URL is used for obtaining samlidp metadata

metadataRefreshInterval Interval in minute for fetching metadata from specified metadata URL

metadataImportStatus Describes metadata import status.

signatureService Name of the service in cloud used to sign the data

samlSigningCertVersion version of the certificate in signature service used to sign the SAMLResposne that is sent to Relying Party or Service Provider after successful authentication

samlSPCertVersion version of the certificate in signature service used to verify the signature of the incoming AuthnRequest from a Relying Party or Service Provider

acsUrlRule Expression that will be evaluated to allow Assertion Consumer Service URI coming in the SAML Request

devno count stateflag

rm authentication samlIdPProfile

Deletes an existing saml IdP profile.

Synopsis

rm authentication samlIdPProfile <name>

Arguments

name Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

unset authentication samlIdPProfile

Use this command to remove authentication samlIdPProfile settings.Refer to the set authentication samlIdPProfile command for meanings of the arguments.

Synopsis

unset authentication samlIdPProfile <name>

add authentication samlIdPProfile

Creates a SAML single IdP profile. This profile is used in verifying incoming authentication request from Service Provider and creating and signing Assertion that is sent to the same.

Synopsis

add authentication samlIdPProfile <name> [(-samlSPCertName <string> [-encryptAssertion (ON | OFF)]) | (-metadataUrl <string>)] [-Attribute1 <string> -Attribute1Expr <string>] [-Attribute2 <string> -Attribute2Expr <string>] [-Attribute3 <string> -Attribute3Expr <string>] [-Attribute4 <string> -Attribute4Expr <string>] [-Attribute5 <string> -Attribute5Expr <string>] [-Attribute6

<string> -Attribute6Expr <string>] [-Attribute7 <string> -Attribute7Expr <string>] [-Attribute8 <string> -Attribute8Expr <string>] [-Attribute9 <string> -Attribute9Expr <string>] [-Attribute10 <string> -Attribute10Expr <string>] [-Attribute11 <string> -Attribute11Expr <string>] [-Attribute12 <string> -Attribute12Expr <string>] [-Attribute13 <string> -Attribute13Expr <string>] [-Attribute14 <string> -Attribute14Expr <string>] [-Attribute15 <string> -Attribute15Expr <string>] [-Attribute16 <string> -Attribute16Expr <string>]

Arguments

name Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

samlSPCertName Name of the SSL certificate of SAML Relying Party. This certificate is used to verify signature of the incoming AuthnRequest from a Relying Party or Service Provider

samlIdPCertName Name of the certificate used to sign the SAMLResposne that is sent to Relying Party or Service Provider after successful authentication

assertionConsumerServiceURL URL to which the assertion is to be sent.

samlIssuerName The name to be used in requests sent fromCitrix ADC to IdP to uniquely identify Citrix ADC.

rejectUnsignedRequests Option to Reject unsigned SAML Requests. ON option denies any authentication requests that arrive without signature.

Possible values: ON, OFF Default value: ON

signatureAlg Algorithm to be used to sign/verify SAML transactions

Possible values: RSA-SHA1, RSA-SHA256 Default value: RSA-SHA256

digestMethod Algorithm to be used to compute/verify digest for SAML transactions

Possible values: SHA1, SHA256 Default value: SHA256

audience Audience for which assertion sent by IdP is applicable. This is typically entity name or url that represents ServiceProvider

NameIDFormat Format of Name Identifier sent in Assertion.

Possible values: Unspecified, emailAddress, X509SubjectName, WindowsDomainQualifiedName, kerberos, entity, persistent, transient Default value: transient

NameIDExpr Expression that will be evaluated to obtain NameIdentifier to be sent in assertion

Attribute1 Name of attribute1 that needs to be sent in SAML Assertion

Attribute1Expr Expression that will be evaluated to obtain attribute1's value to be sent in Assertion

Attribute1FriendlyName User-Friendly Name of attribute1 that needs to be sent in SAML Assertion

Attribute1Format Format of Attribute1 to be sent in Assertion.

Possible values: URI, Basic

Attribute2 Name of attribute2 that needs to be sent in SAML Assertion

Attribute2Expr Expression that will be evaluated to obtain attribute2's value to be sent in Assertion

Attribute2FriendlyName User-Friendly Name of attribute2 that needs to be sent in SAML Assertion

Attribute2Format Format of Attribute2 to be sent in Assertion.

Possible values: URI, Basic

Attribute3 Name of attribute3 that needs to be sent in SAML Assertion

Attribute3Expr Expression that will be evaluated to obtain attribute3's value to be sent in Assertion

Attribute3FriendlyName User-Friendly Name of attribute3 that needs to be sent in SAML Assertion

Attribute3Format Format of Attribute3 to be sent in Assertion.

Possible values: URI, Basic

Attribute4 Name of attribute4 that needs to be sent in SAML Assertion

Attribute4Expr Expression that will be evaluated to obtain attribute4's value to be sent in Assertion

Attribute4FriendlyName User-Friendly Name of attribute4 that needs to be sent in SAML Assertion

Attribute4Format Format of Attribute4 to be sent in Assertion.

Possible values: URI, Basic

Attribute5 Name of attribute5 that needs to be sent in SAML Assertion

Attribute5Expr Expression that will be evaluated to obtain attribute5's value to be sent in Assertion

Attribute5FriendlyName User-Friendly Name of attribute5 that needs to be sent in SAML Assertion

Attribute5Format Format of Attribute5 to be sent in Assertion.

Possible values: URI, Basic

Attribute6 Name of attribute6 that needs to be sent in SAML Assertion

Attribute6Expr Expression that will be evaluated to obtain attribute6's value to be sent in Assertion

Attribute6FriendlyName User-Friendly Name of attribute6 that needs to be sent in SAML Assertion

Attribute6Format Format of Attribute6 to be sent in Assertion.

Possible values: URI, Basic

Attribute7 Name of attribute7 that needs to be sent in SAML Assertion

Attribute7Expr Expression that will be evaluated to obtain attribute7's value to be sent in Assertion

Attribute7FriendlyName User-Friendly Name of attribute7 that needs to be sent in SAML Assertion

Attribute7Format Format of Attribute7 to be sent in Assertion.

Possible values: URI, Basic

Attribute8 Name of attribute8 that needs to be sent in SAML Assertion

Attribute8Expr Expression that will be evaluated to obtain attribute8's value to be sent in Assertion

Attribute8FriendlyName User-Friendly Name of attribute8 that needs to be sent in SAML Assertion

Attribute8Format Format of Attribute8 to be sent in Assertion.

Possible values: URI, Basic

Attribute9 Name of attribute9 that needs to be sent in SAML Assertion

Attribute9Expr Expression that will be evaluated to obtain attribute9's value to be sent in Assertion

Attribute9FriendlyName User-Friendly Name of attribute9 that needs to be sent in SAML Assertion

Attribute9Format Format of Attribute9 to be sent in Assertion.

Possible values: URI, Basic

Attribute10 Name of attribute10 that needs to be sent in SAML Assertion

Attribute10Expr Expression that will be evaluated to obtain attribute10's value to be sent in Assertion

Attribute10FriendlyName User-Friendly Name of attribute10 that needs to be sent in SAML Assertion

Attribute10Format Format of Attribute10 to be sent in Assertion.

Possible values: URI, Basic

Attribute11 Name of attribute11 that needs to be sent in SAML Assertion

Attribute11Expr Expression that will be evaluated to obtain attribute11's value to be sent in Assertion

Attribute11FriendlyName User-Friendly Name of attribute11 that needs to be sent in SAML Assertion

Attribute11Format Format of Attribute11 to be sent in Assertion.

Possible values: URI, Basic

Attribute12 Name of attribute12 that needs to be sent in SAML Assertion

Attribute12Expr Expression that will be evaluated to obtain attribute12's value to be sent in Assertion

Attribute12FriendlyName User-Friendly Name of attribute12 that needs to be sent in SAML Assertion

Attribute12Format Format of Attribute12 to be sent in Assertion.

Possible values: URI, Basic

Attribute13 Name of attribute13 that needs to be sent in SAML Assertion

Attribute13Expr Expression that will be evaluated to obtain attribute13's value to be sent in Assertion

Attribute13FriendlyName User-Friendly Name of attribute13 that needs to be sent in SAML Assertion

Attribute13Format Format of Attribute13 to be sent in Assertion.

Possible values: URI, Basic

Attribute14 Name of attribute14 that needs to be sent in SAML Assertion

Attribute14Expr Expression that will be evaluated to obtain attribute14's value to be sent in Assertion

Attribute14FriendlyName User-Friendly Name of attribute14 that needs to be sent in SAML Assertion

Attribute14Format Format of Attribute14 to be sent in Assertion.

Possible values: URI, Basic

Attribute15 Name of attribute15 that needs to be sent in SAML Assertion

Attribute15Expr Expression that will be evaluated to obtain attribute15's value to be sent in Assertion

Attribute15FriendlyName User-Friendly Name of attribute15 that needs to be sent in SAML Assertion

Attribute15Format Format of Attribute15 to be sent in Assertion.

Possible values: URI, Basic

Attribute16 Name of attribute16 that needs to be sent in SAML Assertion

Attribute16Expr Expression that will be evaluated to obtain attribute16's value to be sent in Assertion

Attribute16FriendlyName User-Friendly Name of attribute16 that needs to be sent in SAML Assertion

Attribute16Format Format of Attribute16 to be sent in Assertion.

Possible values: URI, Basic

encryptAssertion Option to encrypt assertion when Citrix ADC IDP sends one.

Possible values: ON, OFF Default value: OFF

encryptionAlgorithm Algorithm to be used to encrypt SAML assertion

Possible values: DES3, AES128, AES192, AES256 Default value: AES256

samlBinding This element specifies the transport mechanism of saml messages.

Possible values: REDIRECT, POST, ARTIFACT Default value: POST

skewTime This option specifies the number of minutes on either side of current time that the assertion would be valid. For example, if skewTime is 10, then assertion would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all. Default value: 5

serviceProviderID Unique identifier of the Service Provider that sends SAML Request. Citrix ADC will ensure that the Issuer of the SAML Request matches this URI. In case of SP initiated sign-in scenarios, this value must be same as samlIssuerName configured in samlAction.

signAssertion Option to sign portions of assertion when Citrix ADC IDP sends one. Based on the user selection, either Assertion or Response or Both or none can be signed

Possible values: NONE, ASSERTION, RESPONSE, BOTH Default value: ASSERTION

keyTransportAlg Key transport algorithm to be used in encryption of SAML assertion

Possible values: RSA-V1_5, RSA_OAEP Default value: RSA_OAEP

SPLogoutUrl Endpoint on the ServiceProvider (SP) to which logout messages are to be sent

logoutBinding This element specifies the transport mechanism of saml logout messages.

Possible values: REDIRECT, POST Default value: POST

defaultAuthenticationGroup This group will be part of AAA session's internal group list. This will be helpful to admin in Nfactor flow to decide right AAA configuration for Relaying Party. In authentication policy AAA.USER.IS_MEMBER_OF("<default_auth_group>") is way to use this feature.

metadataUrl This URL is used for obtaining samlidp metadata

metadataRefreshInterval Interval in minute for fetching metadata from specified metadata URL Default value: 3600 Minimum value: 0

signatureService Name of the service in cloud used to sign the data

samlSigningCertVersion version of the certificate in signature service used to sign the SAMLResposne that is sent to Relying Party or Service Provider after successful authentication

samlSPCertVersion version of the certificate in signature service used to verify the signature of the incoming AuthnRequest from a Relying Party or Service Provider

acsUrlRule Expression that will be evaluated to allow Assertion Consumer Service URI coming in the SAML Request

authentication-samlPolicy

The following operations can be performed on "authentication-samlPolicy":

rm| set| add| show| unset|

rm authentication samlPolicy

Removes the specified SAML policy.

Synopsis

rm authentication samlPolicy <name>

Arguments

name Name of the policy to remove.

set authentication samlPolicy

Modifies the specified parameters of a SAML policy.

Synopsis

set authentication samlPolicy <name>

Arguments

name Name of the SAML policy to modify.

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the SAML server.

reqAction Name of the SAML authentication action to be performed if the policy matches.

add authentication samlPolicy

Adds a SAML authentication policy. The policy defines the criteria under which the Citrix ADC attempts to authenticate the user with the specified SAML server.

Synopsis

add authentication samlPolicy <name> <rule> <reqAction>

Arguments

name Name for the SAML policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after SAML policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the SAML server.

reqAction Name of the SAML authentication action to be performed if the policy matches.

show authentication samlPolicy

Displays the current settings for the specified SAML policy. If no policy name is provided, displays a list of all SAML policies currently configured on the Citrix ADC.

Synopsis

show authentication samlPolicy

Arguments

name Name of the SAML policy.

Output

rule The name of the new rule associated with the policy.

reqAction The name of the SAML action associated with the policy.

boundTo The entity name to which policy is bound

activePolicy priority bindPolicyType policyType devno count stateflag

unset authentication samlPolicy

Use this command to remove authentication samlPolicy settings.Refer to the set authentication samlPolicy command for meanings of the arguments.

Synopsis

unset authentication samlPolicy <name>

authentication-smartAccessPolicy

The following operations can be performed on "authentication-smartAccessPolicy":

show| unset| rm| set| add|

show authentication smartAccessPolicy

Displays the current settings for the specified Smartaccess policy. If no policy name is provided, displays a list of all Smartaccess policies currently configured on the Citrix ADC.

Synopsis

show authentication smartAccessPolicy

Arguments

name Name of the Smartaccess policy.

Output

rule Name of the Citrix ADC named rule, or an expression.

action Name of the Smartaccess profile to use if the policy matches.

boundTo The entity name to which policy is bound

activePolicy priority hits Number of hits.

bindPolicyType policyType comment Any comments to preserve information about this policy.

devno count stateflag

unset authentication smartAccessPolicy

Removes the comment from an existing Smartaccess policy..Refer to the set authentication smartAccessPolicy command for meanings of the arguments.

Synopsis

unset authentication smartAccessPolicy <name> -comment

rm authentication smartAccessPolicy

Removes an Smartaccess policy.

Synopsis

rm authentication smartAccessPolicy <name>

Arguments

name Name of the Smartaccess policy to remove.

set authentication smartAccessPolicy

Configures the specified Smartaccess policy.

Synopsis

set authentication smartAccessPolicy <name>

Arguments

name Name of the Smartaccess policy.

rule The new rule to associate with the policy.

action The new Smartaccess action to associate with the policy.

comment Any comments to preserve information about this policy.

add authentication smartAccessPolicy

Adds an Smartaccess authentication policy.

Synopsis

add authentication smartAccessPolicy <name> -rule <string> -action <string>

Arguments

name Name for the Smartaccess policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after Smartaccess policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

rule Name of the Citrix ADC named rule, or an expression.

action Name of the Smartaccess profile to use if the policy matches.

comment Any comments to preserve information about this policy.

authentication-smartAccessProfile

The following operations can be performed on "authentication-smartAccessProfile":

add| set| show| rm| unset|

add authentication smartAccessProfile

Creates a Smartaccess profile with the given tag name.

Synopsis

add authentication smartAccessProfile <name> -tags <string>

Arguments

name Name of the Smartaccess profile

tags The tag that is associated with Smartaccess profile.

comment Optional comment for the profile.

set authentication smartAccessProfile

Updates the tag name of a Smartaccess profile

Synopsis

set authentication smartAccessProfile <name>

Arguments

name Name of the Smartaccess profile

tags The tag that is associated with Smartaccess profile.

comment Optional comment for the profile.

show authentication smartAccessProfile

Displays information about the specified Smartaccess profile given the name.

Synopsis

show authentication smartAccessProfile

Arguments

name Name of the Smartaccess profile.

Output

tags The tag value that is associated with Smartaccess profile.

comment Optional comment for the profile.

devno count stateflag

rm authentication smartAccessProfile

Deletes an already present Smartaccess profile.

Synopsis

rm authentication smartAccessProfile <name>

Arguments

name Name of the Smartaccess profile.

unset authentication smartAccessProfile

Use this command to remove authentication smartAccessProfile settings.Refer to the set authentication smartAccessProfile command for meanings of the arguments.

Synopsis

unset authentication smartAccessProfile <name> -comment

authentication-storefrontAuthAction

The following operations can be performed on "authentication-storefrontAuthAction":

unset| set| add| show| rm|

unset authentication storefrontAuthAction

Use this command to remove authentication storefrontAuthAction settings.Refer to the set authentication storefrontAuthAction command for meanings of the arguments.

Synopsis

unset authentication storefrontAuthAction <name>

set authentication storefrontAuthAction

Modifies the attributes of an existing storefront authentication action.

Synopsis

set authentication storefrontAuthAction <name>

Arguments

name Name of the action to configure.

serverURL URL of the Storefront server. This is the FQDN of the Storefront server. example: https://storefront.com/. Authentication endpoints are learned dynamically by Gateway.

domain Domain of the server that is used for authentication. If users enter name without domain, this parameter is added to username in the authentication request to server.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

Example

set authentication storefrontAuthAction a1 -serverurl someurl

add authentication storefrontAuthAction

Adds an action to be used for authentication using storefront server.

Synopsis

add authentication storefrontAuthAction <name> -serverURL <URL>

Arguments

name Name for the Storefront Authentication action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the profile is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication action" or 'my authentication action').

serverURL URL of the Storefront server. This is the FQDN of the Storefront server. example: https://storefront.com/. Authentication endpoints are learned dynamically by Gateway.

domain Domain of the server that is used for authentication. If users enter name without domain, this parameter is added to username in the authentication request to server.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

Example

add authentication storefrontAuthAction a -serverurl https://google.com/

show authentication storefrontAuthAction

Displays information about the configured storefront authentication action.

Synopsis

show authentication storefrontAuthAction

Arguments

name Name of the storefront authentication action to display. If a name is not provided, information about all actions is shown.

Output

stateflag serverURL URL of the Storefront server. This is the FQDN of the Storefront server. example: https://storefront.com/. Authentication endpoints are learned dynamically by Gateway.

domain Domain of the server that is used for authentication. If users enter name without domain, this parameter is added to username in the authentication request to server.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

Success Failure devno count

Example

show authentication storefrontAuthAction a1

rm authentication storefrontAuthAction

Removes a storefront authentication action. You cannot remove an action that is used in any part of a policy.

Synopsis

rm authentication storefrontAuthAction <name>

Arguments

name Name of the storefront authentication action to remove.

Example

rm authentication storefrontAuthAction a1

authentication-tacacsAction

The following operations can be performed on "authentication-tacacsAction":

unset| rm| add| set| show|

unset authentication tacacsAction

Use this command to remove authentication tacacsAction settings.Refer to the set authentication tacacsAction command for meanings of the arguments.

Synopsis

unset authentication tacacsAction <name>

rm authentication tacacsAction

Removes a TACACS+ profile (action). A profile cannot be removed as long as it is bound to a policy.

Synopsis

rm authentication tacacsAction <name>

Arguments

name Name of the profile to be removed.

add authentication tacacsAction

Creates an action (profile) for a TACACS+ server. The profile contains all configuration data necessary to communicate with that TACACS+ server.

Synopsis

add authentication tacacsAction <name> {-tacacsSecret }

Arguments

name Name for the TACACS+ profile (action). Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after TACACS profile is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication action" or 'y authentication action').

serverIP IP address assigned to the TACACS+ server.

serverPort Port number on which the TACACS+ server listens for connections. Default value: 49 Minimum value: 1

authTimeout Number of seconds the Citrix ADC waits for a response from the TACACS+ server. Default value: 3 Minimum value: 1

tacacsSecret Key shared between the TACACS+ server and the Citrix ADC. Required for allowing the Citrix ADC to communicate with the TACACS+ server.

authorization Use streaming authorization on the TACACS+ server.

Possible values: ON, OFF

accounting Whether the TACACS+ server is currently accepting accounting messages.

Possible values: ON, OFF

auditFailedCmds The state of the TACACS+ server that will receive accounting messages.

Possible values: ON, OFF

groupAttrName TACACS+ group attribute name. Used for group extraction on the TACACS+ server.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

Attribute1 Name of the custom attribute to be extracted from server and stored at index '1' (where '1' changes for each attribute)

Attribute2 Name of the custom attribute to be extracted from server and stored at index '2' (where '2' changes for each attribute)

Attribute3 Name of the custom attribute to be extracted from server and stored at index '3' (where '3' changes for each attribute)

Attribute4 Name of the custom attribute to be extracted from server and stored at index '4' (where '4' changes for each attribute)

Attribute5 Name of the custom attribute to be extracted from server and stored at index '5' (where '5' changes for each attribute)

Attribute6 Name of the custom attribute to be extracted from server and stored at index '6' (where '6' changes for each attribute)

Attribute7 Name of the custom attribute to be extracted from server and stored at index '7' (where '7' changes for each attribute)

Attribute8 Name of the custom attribute to be extracted from server and stored at index '8' (where '8' changes for each attribute)

Attribute9 Name of the custom attribute to be extracted from server and stored at index '9' (where '9' changes for each attribute)

Attribute10 Name of the custom attribute to be extracted from server and stored at index '10' (where '10' changes for each attribute)

Attribute11 Name of the custom attribute to be extracted from server and stored at index '11' (where '11' changes for each attribute)

Attribute12 Name of the custom attribute to be extracted from server and stored at index '12' (where '12' changes for each attribute)

Attribute13 Name of the custom attribute to be extracted from server and stored at index '13' (where '13' changes for each attribute)

Attribute14 Name of the custom attribute to be extracted from server and stored at index '14' (where '14' changes for each attribute)

Attribute15 Name of the custom attribute to be extracted from server and stored at index '15' (where '15' changes for each attribute)

Attribute16 Name of the custom attribute to be extracted from server and stored at index '16' (where '16' changes for each attribute)

Attributes List of attribute names separated by ',' which needs to be fetched from tacacs server. Note that preceeding and trailing spaces will be removed. Attribute name can be 127 bytes and total length of this string should not cross 2047 bytes. These attributes have multi-value support separated by ',' and stored as key-value pair in AAA session

set authentication tacacsAction

Modifies a TACACS+ server profile (action).

Synopsis

set authentication tacacsAction <name> {-tacacsSecret }

Arguments

name Name of the TACACS+ profile to modify.

serverIP IP address assigned to the TACACS+ server.

serverPort Port number on which the TACACS+ server listens for connections. Default value: 49 Minimum value: 1

authTimeout Number of seconds the Citrix ADC waits for a response from the TACACS+ server. Default value: 3 Minimum value: 1

tacacsSecret Key shared between the TACACS+ server and the Citrix ADC. Required for allowing the Citrix ADC to communicate with the TACACS+ server.

authorization Use streaming authorization on the TACACS+ server.

Possible values: ON, OFF

accounting Whether the TACACS+ server is currently accepting accounting messages.

Possible values: ON, OFF

auditFailedCmds The state of the TACACS+ server that will receive accounting messages.

Possible values: ON, OFF

groupAttrName TACACS+ group attribute name. Used for group extraction on the TACACS+ server.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

Attribute1 Name of the custom attribute to be extracted from server and stored at index '1' (where '1' changes for each attribute)

Attribute2 Name of the custom attribute to be extracted from server and stored at index '2' (where '2' changes for each attribute)

Attribute3 Name of the custom attribute to be extracted from server and stored at index '3' (where '3' changes for each attribute)

Attribute4 Name of the custom attribute to be extracted from server and stored at index '4' (where '4' changes for each attribute)

Attribute5 Name of the custom attribute to be extracted from server and stored at index '5' (where '5' changes for each attribute)

Attribute6 Name of the custom attribute to be extracted from server and stored at index '6' (where '6' changes for each attribute)

Attribute7 Name of the custom attribute to be extracted from server and stored at index '7' (where '7' changes for each attribute)

Attribute8 Name of the custom attribute to be extracted from server and stored at index '8' (where '8' changes for each attribute)

Attribute9 Name of the custom attribute to be extracted from server and stored at index '9' (where '9' changes for each attribute)

Attribute10 Name of the custom attribute to be extracted from server and stored at index '10' (where '10' changes for each attribute)

Attribute11 Name of the custom attribute to be extracted from server and stored at index '11' (where '11' changes for each attribute)

Attribute12 Name of the custom attribute to be extracted from server and stored at index '12' (where '12' changes for each attribute)

Attribute13 Name of the custom attribute to be extracted from server and stored at index '13' (where '13' changes for each attribute)

Attribute14 Name of the custom attribute to be extracted from server and stored at index '14' (where '14' changes for each attribute)

Attribute15 Name of the custom attribute to be extracted from server and stored at index '15' (where '15' changes for each attribute)

Attribute16 Name of the custom attribute to be extracted from server and stored at index '16' (where '16' changes for each attribute)

Attributes List of attribute names separated by ',' which needs to be fetched from tacacs server. Note that preceeding and trailing spaces will be removed. Attribute name can be 127 bytes and total length of this string should not cross 2047 bytes. These attributes have multi-value support separated by ',' and stored as key-value pair in AAA session

show authentication tacacsAction

Displays the current configuration settings for the specified TACACS+ profile (action).

Synopsis

show authentication tacacsAction

Arguments

name Name of the TACACS+ profile.

Output

serverIP IP address assigned to the TACACS+ server.

serverPort Port number on which the TACACS+ server listens for connections.

authTimeout Number of seconds the Citrix ADC waits for a response from the TACACS+ server.

tacacsSecret Key shared between the TACACS+ server and the Citrix ADC. Required for allowing the Citrix ADC to communicate with the TACACS+ server.

authorization Use streaming authorization on the TACACS+ server.

accounting Whether the TACACS+ server is currently accepting accounting messages.

auditFailedCmds The state of the TACACS+ server that will receive accounting messages.

groupAttrName TACACS+ group attribute name. Used for group extraction on the TACACS+ server.

Success Failure defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

stateflag Attribute1 Name of the custom attribute to be extracted from server and stored at index '1' (where '1' changes for each attribute)

Attribute2 Name of the custom attribute to be extracted from server and stored at index '2' (where '2' changes for each attribute)

Attribute3 Name of the custom attribute to be extracted from server and stored at index '3' (where '3' changes for each attribute)

Attribute4 Name of the custom attribute to be extracted from server and stored at index '4' (where '4' changes for each attribute)

Attribute5 Name of the custom attribute to be extracted from server and stored at index '5' (where '5' changes for each attribute)

Attribute6 Name of the custom attribute to be extracted from server and stored at index '6' (where '6' changes for each attribute)

Attribute7 Name of the custom attribute to be extracted from server and stored at index '7' (where '7' changes for each attribute)

Attribute8 Name of the custom attribute to be extracted from server and stored at index '8' (where '8' changes for each attribute)

Attribute9 Name of the custom attribute to be extracted from server and stored at index '9' (where '9' changes for each attribute)

Attribute10 Name of the custom attribute to be extracted from server and stored at index '10' (where '10' changes for each attribute)

Attribute11 Name of the custom attribute to be extracted from server and stored at index '11' (where '11' changes for each attribute)

Attribute12 Name of the custom attribute to be extracted from server and stored at index '12' (where '12' changes for each attribute)

Attribute13 Name of the custom attribute to be extracted from server and stored at index '13' (where '13' changes for each attribute)

Attribute14 Name of the custom attribute to be extracted from server and stored at index '14' (where '14' changes for each attribute)

Attribute15 Name of the custom attribute to be extracted from server and stored at index '15' (where '15' changes for each attribute)

Attribute16 Name of the custom attribute to be extracted from server and stored at index '16' (where '16' changes for each attribute)

Attributes List of attribute names separated by ',' which needs to be fetched from tacacs server. Note that preceeding and trailing spaces will be removed. Attribute name can be 127 bytes and total length of this string should not cross 2047 bytes. These attributes have multi-value support separated by ',' and stored as key-value pair in AAA session

devno count

authentication-tacacsPolicy

The following operations can be performed on "authentication-tacacsPolicy":

unset| set| add| rm| show|

unset authentication tacacsPolicy

Use this command to remove authentication tacacsPolicy settings.Refer to the set authentication tacacsPolicy command for meanings of the arguments.

Synopsis

unset authentication tacacsPolicy <name>

set authentication tacacsPolicy

Configures the specified TACACS+ policy.

Synopsis

set authentication tacacsPolicy <name>

Arguments

name Name of the TACACS+ policy.

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the TACACS+ server.

reqAction Name of the TACACS+ action to perform if the policy matches.

add authentication tacacsPolicy

Adds a TACACS+ authentication policy. The policy defines the criteria under which the Citrix ADC attempts to authenticate the user with the specified TACACS+ server.

Synopsis

add authentication tacacsPolicy <name> <rule>

Arguments

name Name for the TACACS+ policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after TACACS+ policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the TACACS+ server.

reqAction Name of the TACACS+ action to perform if the policy matches.

rm authentication tacacsPolicy

Removes the specified TACACS+ policy.

Synopsis

rm authentication tacacsPolicy <name>

Arguments

name Name of the TACACS+ policy to remove.

show authentication tacacsPolicy

Displays the current settings for the specified TACACS+ policy. If no policy name is provided, displays a list of all TACACS+ policies currently configured on the Citrix ADC.

Synopsis

show authentication tacacsPolicy

Arguments

name Name of the TACACS+ policy.

Output

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the TACACS+ server.

reqAction Name of the TACACS+ action to perform if the policy matches.

boundTo The entity name to which policy is bound

activePolicy priority bindPolicyType policyType devno count stateflag

authentication-vserver

The following operations can be performed on "authentication-vserver":

rm| rename| set| add| show| enable| stat| disable| unbind| unset| bind|

rm authentication vserver

Removes an authentication virtual server.

Synopsis

rm authentication vserver <name>@ ...

Arguments

name Name of the authentication virtual server to remove.

Example

rm vserver authn_vip

rename authentication vserver

Rename an authentication virtual server.

Synopsis

rename authentication vserver <name>@ <newName>@

Arguments

name Current name of the authentication virtual server.

newName New name of the authentication virtual server. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, 'my authentication policy' or "my authentication policy").

Example

rename authentication vserver av1 av_new

set authentication vserver

Modifies the specified parameters of an existing authentication virtual server.

Synopsis

set authentication vserver <name>

Arguments

name Name of the virtual server to modify.

IPAddress IP address of the authentication virtual server, if a single IP address is assigned to the virtual server.

authentication Require users to be authenticated before sending traffic through this virtual server.

Possible values: ON, OFF Default value: ON

comment Any comments associated with this virtual server.

appflowLog Log AppFlow flow information.

Possible values: ENABLED, DISABLED Default value: ENABLED

maxLoginAttempts Maximum Number of login Attempts Minimum value: 1 Maximum value: 255

failedLoginTimeout Number of minutes an account will be locked if user exceeds maximum permissible attempts Minimum value: 1

certkeyNames Name of the certificate key that was bound to the corresponding SSL virtual server as the Certificate Authority for the device certificate

SameSite SameSite attribute value for Cookies generated in AAATM context. This attribute value will be appended only for the cookies which are specified in the builtin patset ns_cookies_samesite

Possible values: None, LAX, STRICT

add authentication vserver

Creates an authentication virtual server.

Synopsis

add authentication vserver <name> <serviceType> [<IPAddress>] [-maxLoginAttempts <positive_integer>]

Arguments

name Name for the new authentication virtual server. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the authentication virtual server is added by using the rename authentication vserver command.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

serviceType Protocol type of the authentication virtual server. Always SSL.

Possible values: SSL Default value: SSL

IPAddress IP address of the authentication virtual server, if a single IP address is assigned to the virtual server.

range If you are creating a series of virtual servers with a range of IP addresses assigned to them, the length of the range. The new range of authentication virtual servers will have IP addresses consecutively numbered, starting with the primary address specified with the IP Address parameter. Default value: 1 Minimum value: 1

port TCP port on which the virtual server accepts connections.

state Initial state of the new virtual server.

Possible values: ENABLED, DISABLED Default value: ENABLED

authentication Require users to be authenticated before sending traffic through this virtual server.

Possible values: ON, OFF Default value: ON

comment Any comments associated with this virtual server.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

appflowLog Log AppFlow flow information.

Possible values: ENABLED, DISABLED Default value: ENABLED

maxLoginAttempts Maximum Number of login Attempts Minimum value: 1 Maximum value: 255

failedLoginTimeout Number of minutes an account will be locked if user exceeds maximum permissible attempts Minimum value: 1

certkeyNames Name of the certificate key that was bound to the corresponding SSL virtual server as the Certificate Authority for the device certificate

SameSite SameSite attribute value for Cookies generated in AAATM context. This attribute value will be appended only for the cookies which are specified in the builtin patset ns_cookies_samesite

Possible values: None, LAX, STRICT

Example

The following example creates an authentication vserver named myauthenticationvip which supports SSL portocol and with AAA functionality enabled: vserver myauthenticationvip SSL 65.219.17.34 443 -aaa ON

show authentication vserver

Displays the configuration of the specified authentication virtual server. If no authentication virtual server is specified, displays a list of all authentication virtual servers that are currently configured on the Citrix ADC.

Synopsis

show authentication vserver show authentication vserver stats - alias for 'stat authentication vserver'

Arguments

name Name of the authentication virtual server.

Output

IPAddress The Virtual IP address of the authentication vserver.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

IPAddress The IP address of the authentication server.

value Indicates whether or not the certificate is bound or if SSL offload is disabled.

port The virtual TCP port of the authentication vserver.

range The range of authentication vserver IP addresses. The new range of authentication vservers will have IP addresses consecutively numbered, starting with the primary address specified with the <ipaddress> argument.

serviceType The authentication vserver's protocol type, Currently the only possible value is SSL.

type The type of Virtual Server, e.g. CONTENT based or ADDRESS based.

state The current state of the Virtual server, e.g. UP, DOWN, BUSY, etc.

status Whether or not this vserver responds to ARPs and whether or not round-robin selection is temporarily in effect.

cacheType Virtual server's cache type. The options are: TRANSPARENT, REVERSE and FORWARD.

redirect The cache redirect policy. The valid redirect policies are: l.CACHE - Directs all requests to the cache. 2.POLICY - Applies cache redirection policy to determine whether the request should be directed to the cache or origin. This is the default setting. 3.ORIGIN - Directs all requests to the origin server.

precedence This argument is used only when configuring content switching on the specified virtual server. This is applicable only if both the URL and RULE-based policies have been configured on the same virtual server. It specifies the type of policy (URL or RULE) that takes precedence on the content switching virtual server. The default setting is RULE. lURL - In this case, the incoming request is matched against the URL-based policies before the rule-based policies. lRULE - In this case, the incoming request is matched against the rule-based policies before the URL-based policies. For all URL-based policies, the precedence hierarchy is: 1.Domain and exact URL 2.Domain, prefix and suffix 3.Domain and suffix 4.Domain and prefix 5.Domain only 6.Exact URL 7.Prefix and suffix 8.Suffix only 9.Prefix only 10.Default

redirectURL The URL where traffic is redirected if the virtual server in system becomes unavailable. WARNING!Make sure that the domain you specify in the URL does not match the domain specified in the -d domainName argument of the ###add cs policy### command. If the same domain is specified in both arguments, the request will be continuously redirected to the same unavailable virtual server in the system. If so, the user may not get the requested content.

authentication Indicates whether or not authentication is being applied to incoming users to the VPN.

curAAAUsers The number of current users logged in to this vserver.

AuthenticationDomain The domain of the authentication cookie set by Authentication vserver

policyName The name of the policy, if any, bound to the authentication vserver.

policy The name of the policy, if any, bound to the authentication vserver.

serviceName The name of the service, if any, to which the vserver policy is bound.

weight Weight for this service, if any. This weight is used when the system performs load balancing, giving greater priority to a specific service. It is useful when the services bound to a virtual server are of different capacity.

cacheVserver The name of the default target cache virtual server, if any, to which requests are redirected.

backupVServer The name of the backup vpn virtual server for this vpn virtual server.

cltTimeout The idle time, if any, in seconds after which the client connection is terminated.

soMethod VPN client applications are allocated from a block of Intranet IP addresses. That block may be exhausted after a certain number of connections. This switch specifies the method used to determine whether or not a new connection will spillover, or exhaust, the allocated block of Intranet IP addresses for that application. Possible values are CONNECTION or DYNAMICCONNECTION. CONNECTION means that a static integer value is the hard limit for the spillover threshold. The spillover threshold is described below. DYNAMICCONNECTION means that the spillover threshold is set according to the maximum number of connections defined for the vpn vserver.

soThreshold VPN client applications are allocated from a block of Intranet IP addresses. That block may be exhausted after a certain number of connections. The value of this option is number of client connections after which the Mapped IP address is used as the client source IP address instead of an address from the allocated block of Intranet IP addresses.

soPersistence Whether or not cookie-based site persistance is enabled for this VPN vserver. Possible values are 'ConnectionProxy', HTTPRedirect, or NONE

soPersistenceTimeOut The timeout, if any, for cookie-based site persistance of this VPN vserver.

priority The priority, if any, of the vpn vserver policy.

downStateFlush Perform delayed clean up of connections on this vserver.

type Bindpoint to which the policy is bound.

actType disablePrimaryOnDown Tells whether traffic will continue reaching backup vservers even after primary comes UP from DOWN state.

Listenpolicy Listenpolicy configured for authentication vserver

Listenpriority Priority of listen policy for authentication vserver

tcpProfileName The name of the TCP profile.

httpProfileName Name of the HTTP profile.

comment Any comments associated with this virtual server.

policySubType stateflag flags appflowLog Log AppFlow flow information.

vstype Virtual Server Type, e.g. Load Balancing, Content Switch, Cache Redirection

state Initial state of the new virtual server.

ngname Nodegroup devno to which this authentication vsever belongs to

maxLoginAttempts Maximum Number of login Attempts

failedLoginTimeout Number of minutes an account will be locked if user exceeds maximum permissible attempts

secondary Bind the authentication policy to the secondary chain. Provides for multifactor authentication in which a user must authenticate via both a primary authentication method and, afterward, via a secondary authentication method. Because user groups are aggregated across authentication systems, usernames must be the same on all authentication servers. Passwords can be different.

groupExtraction Bind the Authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.

nextFactor On success invoke label.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

portaltheme Theme for Authentication virtual server Login portal

noDefaultBindings to determine if the configuration will have default ssl CIPHER and ECC curve bindings

certkeyNames Name of the certificate key that was bound to the corresponding SSL virtual server as the Certificate Authority for the device certificate

SameSite SameSite attribute value for Cookies generated in AAATM context. This attribute value will be appended only for the cookies which are specified in the builtin patset ns_cookies_samesite

devno count

Example

show authentication vserver

enable authentication vserver

Enables an authentication virtual server that is disabled. Note: Virtual servers, when added, are normally enabled by default.

Synopsis

enable authentication vserver <name>@

Arguments

name Name of the virtual server to enable.

Example

enable vserver authentication1

stat authentication vserver

Displays statistics about the specified authentication virtual server. If no authentication virtual server is specified, displays statistics for all authentication virtual servers that are currently configured on the Citrix ADC.

Synopsis

stat authentication vserver

Arguments

name Name of the authentication virtual server.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

IP address (IP) The IP address on which the service is running.

Port (port) The port on which the service is running.

Vserver protocol (Protocol) Protocol associated with the vserver

State Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)

Requests (Req) Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Responses (Rsp) Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Request bytes (Reqb) Total number of request bytes received on this service or virtual server.

Response bytes (Rspb) Number of response bytes received by this service or virtual server.

Related Commands

- stat authentication OAuthIdPPolicy

disable authentication vserver

Disables an authentication virtual server, taking it out of service.

Synopsis

disable authentication vserver <name>@

Arguments

name Name of the virtual server to disable. Notes:

1. The Citrix ADC still responds to ARP and/or ping requests for the IP address of disabled virtual servers.
2. Because the virtual server configuration still exists on the Citrix ADC, you can reenable the virtual server.

Example

disable vserver authn_vip

unbind authentication vserver

Unbinds the specified policy from the specified authentication virtual server.

Synopsis

unbind authentication vserver <name> [-policy <string>]

Arguments

name Name of the virtual server.

policy Name of the policy to be unbound.

secondary Applicable only to classic authentication policy

groupExtraction Applicable only to classic authentication policy

type Bind point from which to unbind the policy.

Possible values: REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE

portaltheme Name of Theme to be unbound from authentication vserver

unset authentication vserver

Removes the settings of an existing authentication virtual server. Attributes for which a default value is available revert to their default values. Refer to the set authentication vserver command for

descriptions of the parameters..Refer to the set authentication vserver command for meanings of the arguments.

Synopsis

unset authentication vserver <name>

bind authentication vserver

Binds authentication policies to an authentication virtual server.

Synopsis

bind authentication vserver <name> [-policy <string>]

Arguments

name Name of the authentication virtual server to which to bind the policy.

policy Name of the policy to bind to the virtual server.

priority Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Policies are evaluated in the order of their priorities, and the first policy that matches the request is applied. Must be unique within the list of policies bound to the authentication virtual server.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, 'my authentication policy' or "my authentication policy"). Minimum value: 0

secondary Applicable only while bindind classic authentication policy as advance authentication policy use nFactor

groupExtraction Applicable only while bindind classic authentication policy as advance authentication policy use nFactor

nextFactor Applicable only while binding advance authentication policy as classic authentication policy does not support nFactor

gotoPriorityExpression Applicable only to advance authentication policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.

- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

type Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression.

Possible values: REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE

portaltheme Portal theme to be bound to Authentication vserver

authentication-webAuthAction

The following operations can be performed on "authentication-webAuthAction":

set| rm| add| unset| show|

set authentication webAuthAction

Modifies the attributes of an existing web authentication action.

Synopsis

set authentication webAuthAction <name>

Arguments

name Name of the action to configure.

serverIP IP address of the web server to be used for authentication.

serverPort Port on which the web server accepts connections. Minimum value: 1

fullReqExpr Exact HTTP request, in the form of an expression, which the Citrix ADC sends to the authentication server. The Citrix ADC does not check the validity of this request. One must manually validate the request.

scheme Type of scheme for the web server.

Possible values: http, https

successRule Expression, that checks to see if authentication is successful.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

Attribute1 Expression that would be evaluated to extract attribute1 from the webauth response

Attribute2 Expression that would be evaluated to extract attribute2 from the webauth response

Attribute3 Expression that would be evaluated to extract attribute3 from the webauth response

Attribute4 Expression that would be evaluated to extract attribute4 from the webauth response

Attribute5 Expression that would be evaluated to extract attribute5 from the webauth response

Attribute6 Expression that would be evaluated to extract attribute6 from the webauth response

Attribute7 Expression that would be evaluated to extract attribute7 from the webauth response

Attribute8 Expression that would be evaluated to extract attribute8 from the webauth response

Attribute9 Expression that would be evaluated to extract attribute9 from the webauth response

Attribute10 Expression that would be evaluated to extract attribute10 from the webauth response

Attribute11 Expression that would be evaluated to extract attribute11 from the webauth response

Attribute12 Expression that would be evaluated to extract attribute12 from the webauth response

Attribute13 Expression that would be evaluated to extract attribute13 from the webauth response

Attribute14 Expression that would be evaluated to extract attribute14 from the webauth response

Attribute15 Expression that would be evaluated to extract attribute15 from the webauth response

Attribute16 Expression that would be evaluated to extract attribute16 from the webauth response

Example

set authentication webAuthAction a1 -ServerIP 1.1.1.1 -ServerPort 80

rm authentication webAuthAction

Removes a web authentication action. You cannot remove an action that is used in any part of a policy.

Synopsis

rm authentication webAuthAction <name>

Arguments

name Name of the web authentication action to remove.

Example

rm authentication webAuthAction a1

add authentication webAuthAction

Adds an action to be used for web authentication.

- Specify the entire HTTP request in a single expression.

Synopsis

add authentication webAuthAction <name> -serverIP <ip_addr|ipv6_addr|> *-serverPort <port|>* -scheme (http | https) -successRule <expression>

Arguments

name Name for the Web Authentication action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the profile is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication action" or 'my authentication action').

serverIP IP address of the web server to be used for authentication.

serverPort Port on which the web server accepts connections. Minimum value: 1

fullReqExpr Exact HTTP request, in the form of an expression, which the Citrix ADC sends to the authentication server. The Citrix ADC does not check the validity of this request. One must manually validate the request.

scheme Type of scheme for the web server.

Possible values: http, https

successRule Expression, that checks to see if authentication is successful.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

Attribute1 Expression that would be evaluated to extract attribute1 from the webauth response

Attribute2 Expression that would be evaluated to extract attribute2 from the webauth response

Attribute3 Expression that would be evaluated to extract attribute3 from the webauth response

Attribute4 Expression that would be evaluated to extract attribute4 from the webauth response

Attribute5 Expression that would be evaluated to extract attribute5 from the webauth response

Attribute6 Expression that would be evaluated to extract attribute6 from the webauth response

Attribute7 Expression that would be evaluated to extract attribute7 from the webauth response

Attribute8 Expression that would be evaluated to extract attribute8 from the webauth response

Attribute9 Expression that would be evaluated to extract attribute9 from the webauth response

Attribute10 Expression that would be evaluated to extract attribute10 from the webauth response

Attribute11 Expression that would be evaluated to extract attribute11 from the webauth response

Attribute12 Expression that would be evaluated to extract attribute12 from the webauth response

Attribute13 Expression that would be evaluated to extract attribute13 from the webauth response

Attribute14 Expression that would be evaluated to extract attribute14 from the webauth response

Attribute15 Expression that would be evaluated to extract attribute15 from the webauth response

Attribute16 Expression that would be evaluated to extract attribute16 from the webauth response

Example

add authentication webAuthAction a1 -ServerIP 1.1.1.1 -ServerPort 80 -scheme HTTP -successRule true -fullReqExpr <http request string>

unset authentication webAuthAction

Use this command to remove authentication webAuthAction settings.Refer to the set authentication webAuthAction command for meanings of the arguments.

Synopsis

unset authentication webAuthAction <name>

show authentication webAuthAction

Displays information about the configured web authentication action.

Synopsis

show authentication webAuthAction

Arguments

name Name of the web authentication action to display. If a name is not provided, information about all actions is shown.

Output

stateflag serverIP IP address of the web server to be used for authentication.

serverPort Port on which the web server accepts connections.

fullReqExpr Exact HTTP request, in the form of an expression, which the Citrix ADC sends to the authentication server. The Citrix ADC does not check the validity of this request. One must manually validate the request.

scheme Type of scheme for the web server.

successRule Expression, that checks to see if authentication is successful.

defaultAuthenticationGroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

Attribute1 Expression that would be evaluated to extract attribute1 from the webauth response

Attribute2 Expression that would be evaluated to extract attribute2 from the webauth response

Attribute3 Expression that would be evaluated to extract attribute3 from the webauth response

Attribute4 Expression that would be evaluated to extract attribute4 from the webauth response

Attribute5 Expression that would be evaluated to extract attribute5 from the webauth response

Attribute6 Expression that would be evaluated to extract attribute6 from the webauth response

Attribute7 Expression that would be evaluated to extract attribute7 from the webauth response

Attribute8 Expression that would be evaluated to extract attribute8 from the webauth response

Attribute9 Expression that would be evaluated to extract attribute9 from the webauth response

Attribute10 Expression that would be evaluated to extract attribute10 from the webauth response

Attribute11 Expression that would be evaluated to extract attribute11 from the webauth response

Attribute12 Expression that would be evaluated to extract attribute12 from the webauth response

Attribute13 Expression that would be evaluated to extract attribute13 from the webauth response

Attribute14 Expression that would be evaluated to extract attribute14 from the webauth response

Attribute15 Expression that would be evaluated to extract attribute15 from the webauth response

Attribute16 Expression that would be evaluated to extract attribute16 from the webauth response

devno count

Example

show authentication webAuthAction a1

authentication-webAuthPolicy

The following operations can be performed on "authentication-webAuthPolicy":

rm| show| set| add|

rm authentication webAuthPolicy

Removes an WebAuth policy.

Synopsis

rm authentication webAuthPolicy <name>

Arguments

name Name of the WebAuth policy to remove.

show authentication webAuthPolicy

Displays the current settings for the specified WebAuth policy. If no policy name is provided, displays a list of all WebAuth policies currently configured on the Citrix ADC.

Synopsis

show authentication webAuthPolicy

Arguments

name Name of the WebAuth policy.

Output

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the Web server.

action Name of the WebAuth action to perform if the policy matches.

boundTo The entity name to which policy is bound

activePolicy priority bindPolicyType policyType devno count stateflag

set authentication webAuthPolicy

Configures the specified WebAuth policy.

Synopsis

set authentication webAuthPolicy <name>

Arguments

name Name of the WebAuth policy.

rule The new rule to associate with the policy.

action The new WebAuth action to associate with the policy.

add authentication webAuthPolicy

Adds an WebAuth authentication policy. The policy defines the criteria under which the Citrix ADC attempts to authenticate the user with the specified Web server.

Synopsis

add authentication webAuthPolicy <name> -rule <string> -action <string>

Arguments

name Name for the WebAuth policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after LDAP policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the Web server.

action Name of the WebAuth action to perform if the policy matches.

authorization

authorization-action

The following operations can be performed on "authorization-action":

show authorization action

Show details of authorization actions.

Synopsis

show authorization action

Arguments

name Name of authorization action

Output

devno count stateflag

Authorization

The entities on which you can perform NetScaler CLI operations:

- authorization-action
- authorization-policy
- authorization-policylabel

authorization-policy

The following operations can be performed on "authorization-policy":

set| rename| add| rm| show|

set authorization policy

Configures the specified parameters of an authorization policy.

Synopsis

set authorization policy <name>

Arguments

name Name of the authorization policy to modify.

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to perform the authentication.

action Action to perform if the policy matches: either allow or deny the request.

rename authorization policy

Rename a author policy.

Synopsis

rename authorization policy <name>@ <newName>@

Arguments

name The name of the author policy.

newName The new name of the author policy.

Example

rename auth policy oldname newname

add authorization policy

Creates an authorization policy. Authorization policies allow AAA users and AAA groups to access resources through SSL VPN/AAA-TM enabled virtual servers.

Synopsis

add authorization policy <name> <rule> <action>

Arguments

name Name for the new authorization policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the authorization policy is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authorization policy" or 'my authorization policy').

rule Name of the Citrix ADC named rule, or an expression, that the policy uses to perform the authentication.

action Action to perform if the policy matches: either allow or deny the request.

Example

Example: Consider the following authorization policy, "author-policy",

add authorization policy author-policy "URL == /*.gif" DENY bind aaa user foo -policy author-policy

If the user "foo" now logs in through the SSL VPN and makes any other request except "gif", the rule will be evaluated to FALSE, and the negetion of DENY, i.e. ALLOW, will be applied. So all those resource will implicitly be allowed to access. If "foo" tries to accesss "abc.gif" this access will be denied.

rm authorization policy

Removes an authorization policy.

Synopsis

rm authorization policy <name>

Arguments

name Name of the authorization policy to be removed.

show authorization policy

Displays the current settings for the specified authorization policy. If no policy name is provided, displays a list of all authorization policies currently configured on the Citrix ADC.

Synopsis

show authorization policy

Arguments

name Name of the authorization policy.

Output

rule Rule of the policy.

action Authorization action associated with the policy. It can be either ALLOW or DENY.

boundTo The entity name to which policy is bound

activePolicy Indicates whether policy is bound or not.

priority flag bindPolicyType policyType vserverType expressionType Type of policy (Classic/ Advanced)

hits Number of hits.

type devno count stateflag

authorization-policylabel

The following operations can be performed on "authorization-policylabel":

bind| show| rename| rm| stat| unbind| add|

bind authorization policylabel

Binds an authorization policy to a label.

Synopsis

bind authorization policylabel <labelName> <policyName> <priority>

Arguments

labelName Name of the authorization policy label to which to bind the policy.

policyName Name of the authorization policy to bind to the policy label.

priority Positive integer specifying the priority of the policy. The lower the number, the higher the priority. Policies within a label are evaluated in the order of their priority numbers. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.

- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is smaller than the current policy's priority number.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then either forward the request or response to the specified virtual server or evaluate the specified policy label.

labelType Type of invocation. Available settings function as follows:

- reqvserver - Send the request to the specified request virtual server.
- resvserver - Send the response to the specified response virtual server.
- policylabel - Invoke the specified policy label.

Possible values: reqvserver, resvserver, policylabel

labelName Name of the policy label to invoke if the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is set to Policy Label.

Example

i)bind authorization policylabel trans_http_url pol_1 1 2 -invoke reqvserver CURRENT ii)bind authorization policylabel trans_http_url pol_2 2

show authorization policylabel

Displays the current settings for the specified authorization policy label. If no policy name is provided, displays a list of all authorization policy labels currently configured on the Citrix ADC.

Synopsis

show authorization policylabel

Arguments

labelName Name of the authorization policy label.

Output

stateflag numpol Number of polices bound to label.

hits Number of times policy label was invoked.

policyName Name of the authorization policy to bind to the policy label.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType Type of invocation. Available settings function as follows:

- reqvserver - Send the request to the specified request virtual server.
- resvserver - Send the response to the specified response virtual server.
- policylabel - Invoke the specified policy label.

labelName Name of the policy label to invoke if the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is set to Policy Label.

flowType Flowtype of the bound authorization policy.

description Description of the policylabel

flags devno count

Example

i)show authorization policylabel trans_http_url ii)show authorization policylabel

rename authorization policylabel

Rename a auth policy label.

Synopsis

rename authorization policylabel <labelName>@ <newName>@

Arguments

labelName The name of the auth policy label

newName The new name of the auth policy label

Example

rename auth policy label oldname newname

rm authorization policylabel

Removes an authorization policy label.

Synopsis

rm authorization policylabel <labelName>

Arguments

labelName Name of the authorization policy label to remove.

Example

rm authorization policylabel trans_http_url

stat authorization policylabel

Displays statistics for the specified authorization policy label. If no authorization policy label is specified, displays a list of all authorization policy labels.

Synopsis

stat authorization policylabel

Arguments

labelName Name of the authorization policy label.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy Label Hits (Hits) Number of times policy label was invoked.

unbind authorization policylabel

Unbinds the specified policy from the specified authorization policy label.

Synopsis

unbind authorization policylabel <labelName> <policyName>

Arguments

labelName Name for the new authorization policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the authorization policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authorization policy label" or 'authorization policy label').

policyName Name of the authorization policy to bind to the policy label.

priority Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind authorization policylabel trans_http_url pol_1

add authorization policylabel

Creates a user-defined authorization policy label.

Synopsis

add authorization policylabel <labelName>

Arguments

labelName Name for the new authorization policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the authorization policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authorization policy label" or 'authorization policy label').

Example

add authorization policylabel trans_http_url

autoscale

autoscale-action

The following operations can be performed on "autoscale-action":

add| rm| set| unset| show|

add autoscale action

Create a AutoScale action.

Synopsis

add autoscale action <name> -type (SCALE_UP | SCALE_DOWN) -profileName <string> -parameters <string> -vServer <string>

Arguments

name ActionScale action name.

type The type of action.

Possible values: SCALE_UP, SCALE_DOWN

profileName AutoScale profile name.

parameters Parameters to use in the action

vmDestroyGracePeriod Time in minutes a VM is kept in inactive state before destroying Default value: 10 Minimum value: 0

quietTime Time in seconds no other policy is evaluated or action is taken Default value: 300 Minimum value: 0

vServer Name of the vserver on which autoscale action has to be taken.

rm autoscale action

Remove a AutoScale action.

Synopsis

rm autoscale action <name>

Arguments

name ActionScale action name.

set autoscale action

Set a AutoScale action.

Synopsis

set autoscale action <name>

Arguments

name ActionScale action name.

profileName AutoScale profile name.

parameters Parameters to use in the action

vmDestroyGracePeriod Time in minutes a VM is kept in inactive state before destroying Default value: 10 Minimum value: 0

quietTime Time in seconds no other policy is evaluated or action is taken Default value: 300 Minimum value: 0

vServer Name of the vserver on which autoscale action has to be taken.

unset autoscale action

Use this command to remove autoscale action settings.Refer to the set autoscale action command for meanings of the arguments.

Synopsis

unset autoscale action <name>

show autoscale action

Display the autoscale actions.

Synopsis

show autoscale action

Arguments

name ActionScale action name.

Output

type The type of action.

profileName AutoScale profile name.

parameters Parameters to use in the action

vmDestroyGracePeriod Time in minutes a VM is kept in inactive state before destroying

quietTime Time in seconds no other policy is evaluated or action is taken

vServer Name of the vserver on which autoscale action has to be taken.

destIP IP Address on which provisioning server daemon is running

destPort Port on which provisioning server daemon is running

devno count stateflag

Autoscale

The entities on which you can perform NetScaler CLI operations:

autoscale-policy

The following operations can be performed on "autoscale-policy":

rename| unset| set| rm| show| stat| add|

rename autoscale policy

Rename a autoscale policy.

Synopsis

rename autoscale policy <name>@ <newName>@

Arguments

name The name of the autoscale policy.

newName The new name of the autoscale policy.

Example

rename autoscale policy oldname newname

unset autoscale policy

Unset comment/logaction for existing autoscale policy..Refer to the set autoscale policy command for meanings of the arguments.

Synopsis

unset autoscale policy <name>

Example

unset autoscale policy pol9 -undefAction

set autoscale policy

Set a new rule/action/comment for an existing autoscale policy.

Synopsis

set autoscale policy <name>

Arguments

name The name of the autoscale policy.

rule The rule associated with the policy.

action The autoscale profile associated with the policy.

comment Comments associated with this autoscale policy.

logAction The log action associated with the autoscale policy

Example

set autoscaler policy pol -rule true

rm autoscale policy

Remove a autoscale policy.

Synopsis

rm autoscale policy <name>

Arguments

name The name of the autoscale policy.

Example

rm autoscale policy pol

show autoscale policy

Display the autoscale policies.

Synopsis

show autoscale policy

Arguments

name The name of the autoscale policy.

Output

rule The rule associated with the policy.

action The autoscale profile associated with the policy.

comment Comments associated with this autoscale policy.

logAction The log action associated with the autoscale policy

activePolicy Indicates whether policy is bound or not.

stateflag hits Number of hits.

undefHits Number of Undef hits.

priority Specifies the priority of the policy.

boundTo Location where policy is bound

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

devno count

stat autoscale policy

Display autoscale policy statistics.

Synopsis

stat autoscale policy

Arguments

name The name of the autoscale policy for which statistics will be displayed. If not given statistics are shown for all autoscale policies.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Policy undef hits (Undefhits) Number of undef hits on the policy

Example

stat autoscale policy

add autoscale policy

Create a autoscale policy.

Synopsis

add autoscale policy <name> -rule <expression> -action <string>

Arguments

name The name of the autoscale policy.

rule The rule associated with the policy.

action The autoscale profile associated with the policy.

comment Comments associated with this autoscale policy.

logAction The log action associated with the autoscale policy

autoscale-profile

The following operations can be performed on "autoscale-profile":

show| add| set| rm|

show autoscale profile

Display the autoscale profile.

Synopsis

show autoscale profile

Arguments

name AutoScale profile name.

Output

type The type of profile.

url URL providing the service

apiKey api key for authentication with service

sharedSecret shared secret for authentication with service

stateflag devno count

add autoscale profile

Create a AutoScale policy.

Synopsis

add autoscale profile <name> -type CLOUDSTACK -url <URL> -apiKey -sharedSecret

Arguments

name AutoScale profile name.

type The type of profile.

Possible values: CLOUDSTACK

url URL providing the service

apiKey api key for authentication with service

sharedSecret shared secret for authentication with service

set autoscale profile

Set a AutoScale policy.

Synopsis

set autoscale profile <name>

Arguments

name AutoScale profile name.

url URL providing the service

apiKey api key for authentication with service

sharedSecret shared secret for authentication with service

rm autoscale profile

Remove a AutoScale policy.

Synopsis

rm autoscale profile <name>

Arguments

name AutoScale profile name.

azure

azure-application

The following operations can be performed on "azure-application":

add| show| rm|

add azure application

Creates an Azure application entity. This entity contains the credentials required to authenticate to Azure Active Directory and obtain the access token.

Synopsis

add azure application <name> -clientID <string> -clientSecret -tenantID <string> -vaultResource <string>

Arguments

name Name for the application. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the application is created.',

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my application" or 'my application').

clientID Application ID that is generated when an application is created in Azure Active Directory using either the Azure CLI or the Azure portal (GUI)

clientSecret Password for the application configured in Azure Active Directory. The password is specified in the Azure CLI or generated in the Azure portal (GUI).

tenantID ID of the directory inside Azure Active Directory in which the application was created

vaultResource Vault resource for which access token is granted. Example : vault.azure.net

tokenEndpoint URL from where access token can be obtained. If the token end point is not specified, the default value is https://login.microsoftonline.com/<tenant id>.

show azure application

Displays information about all configured Azure applications, or displays detailed information about the specified azure application.

Synopsis

show azure application

Arguments

name Name for the application. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the application is created.',

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my application" or 'my application').

Output

clientID Application ID that is generated when an application is created in Azure Active Directory using either the Azure CLI or the Azure portal (GUI)

tokenEndpoint URL from where access token can be obtained. If the token end point is not specified, the default value is https://login.microsoftonline.com/<tenant id>.

tenantID ID of the directory inside Azure Active Directory in which the application was created

vaultResource Vault resource for which access token is granted. Example : vault.azure.net

devno count stateflag

rm azure application

Deletes an existing Azure application entity

Synopsis

rm azure application <name>

Arguments

name Name for the application. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space,

colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the application is created.',

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my application" or 'my application').

Azure

The entities on which you can perform NetScaler CLI operations:

- azure-application
- azure-keyVault

azure-keyVault

The following operations can be performed on "azure-keyVault":

add| rm| show|

add azure keyVault

Creates a Azure key vault object in NetScaler.

Synopsis

add azure keyVault <name> -azureVaultName <string> -azureApplication <string>

Arguments

name Name for the Key Vault. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the Key Vault is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my keyvault" or 'my keyvault').

azureVaultName Name of the Key Vault configured in Azure cloud using either the Azure CLI or the Azure portal (GUI) with complete domain name. Example: Test.vault.azure.net.

azureApplication Name of the Azure Application object created on the ADC appliance. This object will be used for authentication with Azure Active Directory

rm azure keyVault

Deletes an existing Azure key vault.

Synopsis

rm azure keyVault <name>

Arguments

name Name for the Key Vault. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the Key Vault is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my keyvault" or 'my keyvault').

show azure keyVault

Displays information about all configured Azure key vaults, or displays detailed information about the specified vault.

Synopsis

show azure keyVault

Arguments

name Name for the Key Vault. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the Key Vault is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my keyvault" or 'my keyvault').

Output

azureVaultName Name of the Key Vault configured in Azure cloud using either the Azure CLI or the Azure portal (GUI) with complete domain name. Example: Test.vault.azure.net.

azureApplication Name of the Azure Application object created on the ADC appliance. This object will be used for authentication with Azure Active Directory

state Current state of keyvault

devno count stateflag

basic

Basic

The entities on which you can perform NetScaler CLI operations:

- dbsMonitors
- extendedmemoryparam
- location
- locationData
- locationFile
- locationFile6
- locationParameter
- nstrace
- radiusNode
- reporting
- reportingconfig
- server
- service
- serviceGroup
- serviceGroupMember
- servicegroupbindings
- svcbindings
- systemLevelReporting
- uiinternal
- vserver

dbsMonitors

The following operations can be performed on "dbsMonitors":

restart dbsMonitors

Immediately send DNS queries to resolve the domain names of all the domain-based servers configured on the Citrix ADC.

Synopsis

restart dbsMonitors

Example

restart dbsMonitors

extendedmemoryparam

The following operations can be performed on "extendedmemoryparam":

unset| set| show|

unset extendedmemoryparam

Use this command to remove extendedmemoryparam settings.Refer to the set extendedmemoryparam command for meanings of the arguments.

Synopsis

unset extendedmemoryparam -memLimit

set extendedmemoryparam

Modify the global configuration of the extended memory. This configures memory for LSN and Subscriber Session Store Modules.

Synopsis

set extendedmemoryparam -memLimit <MBytes>

Arguments

memLimit Amount of Citrix ADC memory to reserve for the memory used by LSN and Subscriber Session Store feature, in multiples of 2MB.

Note: If you later reduce the value of this parameter, the amount of active memory is not reduced. Changing the configured memory limit can only increase the amount of active memory.

show extendedmemoryparam

Display the global configuration of extendedmemory. LSN and Subscriber Session Stores use this memory configuration.

Synopsis

show extendedmemoryparam

Arguments

Output

memLimitActive The active memory limit for extendedmemory on the system. Active memory limit could be different from configured memory limit. This could happen when memory limit could not be increased due to unavailability, or could not be decreased as it is already in use. This active memory limit configures the current memory limit for LSN and Subscriber Session Store.

maxMemLimit The maximum value of memory limit for extendedmemory on the system. Actual available memory may be less. This is maximum memory that can be utilized by LSN and Subscriber Session Store modules.

memLimit Amount of Citrix ADC memory to reserve for the memory used by LSN and Subscriber Session Store feature, in multiples of 2MB.

Note: If you later reduce the value of this parameter, the amount of active memory is not reduced. Changing the configured memory limit can only increase the amount of active memory.

minRequiredMemory The minimum memory requirement for extendedmemory. This is minimum memory required for LSN and Subscriber Session Store Modules.

location

The following operations can be performed on "location":

rm| show| add|

rm location

Removes a custom location entry from the Citrix ADC.

Synopsis

rm location <IPfrom> <IPto>

Arguments

IPfrom First IP address in the range, in dotted decimal notation.

IPto Last IP address in the range, in dotted decimal notation.

Example

rm location 192.168.100.1 192.168.100.100

show location

Displays all the custom location entries configured on the Citrix ADC, or just the entry for the specified IP address range.

Synopsis

show location

Arguments

IPfrom The qualifiers in dotted notation for the ipaddress. If this value is not specified, all custom entries are displayed.

Output

stateflag IPto The end of the IP address range.

preferredLocation The qualifiers in dotted notation for the ipaddress range.

q1label Least specific location qualifier.

q2label Location qualifier 2.

q3label Location qualifier 3.

q4label Location qualifier 4.

q5label Location qualifier 5.

q6label Most specific location qualifier.

longitude Numerical value, in degrees, specifying the longitude of the geographical location of the IP address-range. Note: Longitude and latitude parameters are used for selecting a service with the static proximity GSLB method. If they are not specified, selection is based on the qualifiers specified for the location.

latitude Numerical value, in degrees, specifying the latitude of the geographical location of the IP address-range. Note: Longitude and latitude parameters are used for selecting a service with the static proximity GSLB method. If they are not specified, selection is based on the qualifiers specified for the location.

devno count

Example

show location

add location

Creates a custom location entry on the Citrix ADC. Custom locations can be used instead of a static location database if the number of locations you need does not exceed 500. Custom locations can also be used to override incorrect entries in the static database, because the appliance searches the static database before it searches the static location database.

Synopsis

add location <IPfrom> <IPto> <preferredLocation> [-longitude <integer>]

Arguments

IPfrom First IP address in the range, in dotted decimal notation.

IPto Last IP address in the range, in dotted decimal notation.

preferredLocation String of qualifiers, in dotted notation, describing the geographical location of the IP address range. Each qualifier is more specific than the one that precedes it, as in continent.country.region.city.isp.organization. For example, "NA.US.CA.San Jose.ATT.citrix". Note: A qualifier that includes a dot (.) or space ( ) must be enclosed in double quotation marks.

longitude Numerical value, in degrees, specifying the longitude of the geographical location of the IP address-range. Note: Longitude and latitude parameters are used for selecting a service with the static proximity GSLB method. If they are not specified, selection is based on the qualifiers specified for the location. Minimum value: -180 Maximum value: 180

latitude Numerical value, in degrees, specifying the latitude of the geographical location of the IP address-range. Note: Longitude and latitude parameters are used for selecting a service with the static proximity GSLB method. If they are not specified, selection is based on the qualifiers specified for the location. Minimum value: -90 Maximum value: 90

Example

Add location 192.168.100.1 192.168.100.100 *.us.ca.san jose

locationData

The following operations can be performed on "locationData":

clear locationData

Clears all location information, including custom and static database entries.

Synopsis

clear locationData

Example

clear locationdata

locationFile

The following operations can be performed on "locationFile":

add| import| rm| show|

add locationFile

Loads the static location database from the specified file.

Synopsis

add locationFile <locationFile>

Arguments

locationFile Name of the location file, with or without absolute path. If the path is not included, the default path (/var/netscaler/locdb) is assumed. In a high availability setup, the static database must be stored in the same location on both Citrix ADCs.

format Format of the location file. Required for the Citrix ADC to identify how to read the location file.

Possible values: netscaler, ip-country, ip-country-isp, ip-country-region-city, ip-country-region-city-isp, geoip-country, geoip-region, geoip-city, geoip-country-org, geoip-country-isp, geoip-city-isp-org
Default value: netscaler

Example

add locationfile /var/nsmap/locationdb -format Citrix ADC

import locationFile

Imports the specified location file to the Citrix ADC, assigns it the specified name.

Synopsis

import locationFile <locationFile> <src>

Arguments

locationFile Name of the location file, with or without absolute path. If the path is not included, the default path (/var/netscaler/locdb) is assumed. In a high availability setup, the static database must be stored in the same location on both Citrix ADCs.

src URL \(protocol, host, path, and file name\) from where the location file will be imported. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

Example

import locationfile locfile_1 http://www.example.com/file_1

rm locationFile

Removes the currently loaded static location database from the Citrix ADC.

Synopsis

rm locationFile

Example

rm locationfile

show locationFile

Displays the name, including the absolute path, and format of the location file currently loaded on the Citrix ADC.

Synopsis

show locationFile

Arguments

Output

locationFile The name of the location file.

format The format of the location file.

Example

show locationfile

locationFile6

The following operations can be performed on "locationFile6":

add| import| rm| show|

add locationFile6

Loads the IPv6 static location database from the specified file.

Synopsis

add locationFile6 <locationFile>

Arguments

locationFile Name of the IPv6 location file, with or without absolute path. If the path is not included, the default path (/var/netscaler/locdb) is assumed. In a high availability setup, the static database must be stored in the same location on both Citrix ADCs.

format Format of the IPv6 location file. Required for the Citrix ADC to identify how to read the location file.

Possible values: netscaler6, geoip-country6 Default value: netscaler6

Example

add locationfile6 /var/nsmap/locationdb -format netscaler6

import locationFile6

Imports the specified location file to the Citrix ADC, assigns it the specified name.

Synopsis

import locationFile6 <locationFile> <src>

Arguments

locationFile Name of the IPv6 location file, with or without absolute path. If the path is not included, the default path (/var/netscaler/locdb) is assumed. In a high availability setup, the static database must be stored in the same location on both Citrix ADCs.

src URL \(protocol, host, path, and file name\) from where the location file will be imported. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

Example

import locationfile6 locfile6_1 http://www.example.com/file_1

rm locationFile6

Removes the currently loaded static location database from the Citrix ADC.

Synopsis

rm locationFile6

Example

rm locationfile6

show locationFile6

Displays the name, including the absolute path, and format of the location file currently loaded on the Citrix ADC.

Synopsis

show locationFile6

Arguments

Output

locationFile The name of the location file.

format The format of the location file.

devno count stateflag

Example

show locationfile6

locationParameter

The following operations can be performed on "locationParameter":

set| unset| show|

set locationParameter

Sets the location parameters used for static-proximity based global server load balancing. Location parameters include up to six qualifiers and a context that specifies how the qualifiers must be interpreted. Each qualifier specifies the location of an IP address range and is more specific than the one that precedes it, as in continent.country.region.city.isp.organization. For example, "NA.US.CA.San Jose.ATT.citrix". Note: A qualifier that includes a dot (.) or space ( ) must be enclosed in double quotation marks.

Synopsis

set locationParameter

Arguments

context Context for describing locations. In geographic context, qualifier labels are assigned by default in the following sequence: Continent.Country.Region.City.ISP.Organization. In custom context, the qualifiers labels can have any meaning that you designate.

Possible values: geographic, custom

q1label Label specifying the meaning of the first qualifier. Can be specified for custom context only.

q2label Label specifying the meaning of the second qualifier. Can be specified for custom context only.

q3label Label specifying the meaning of the third qualifier. Can be specified for custom context only.

q4label Label specifying the meaning of the fourth qualifier. Can be specified for custom context only.

q5label Label specifying the meaning of the fifth qualifier. Can be specified for custom context only.

q6label Label specifying the meaning of the sixth qualifier. Can be specified for custom context only.

matchWildcardtoany Indicates whether wildcard qualifiers should match any other qualifier including non-wildcard while evaluating location based expressions. Possible values: Yes, No, Expression. Yes - Wildcard qualifiers match any other qualifiers. No - Wildcard qualifiers do not match non-wildcard qualifiers, but match other wildcard qualifiers. Expression - Wildcard qualifiers in an expression match any qualifier in an LDNS location, wildcard qualifiers in the LDNS location do not match non-wildcard qualifiers in an expression

Possible values: YES, NO, Expression Default value: NO

Example

set locationparameter -context custom

unset locationParameter

Use this command to remove locationParameter settings.Refer to the set locationParameter command for meanings of the arguments.

Synopsis

unset locationParameter

show locationParameter

Displays current values for the location parameters, which are used for static-proximity based load balancing.

Synopsis

show locationParameter

Arguments

Output

context The context in which a static proximity decision must be made.

q1label The label for the 1st qualifier. These qualifier labels characterize the locations mapped with the IP addresses used to make static proximity decisions.

q2label Label specifying the meaning of the second qualifier. Can be specified for custom context only.

q3label Label specifying the meaning of the third qualifier. Can be specified for custom context only.

q4label Label specifying the meaning of the fourth qualifier. Can be specified for custom context only.

q5label Label specifying the meaning of the fifth qualifier. Can be specified for custom context only.

q6label Label specifying the meaning of the sixth qualifier. Can be specified for custom context only.

locationFile Currently loaded location database file.

format Location file format

custom Number of configured custom locations.

static Number of configured locations in the database file (static locations).

lines Number of lines in the databse files

errors Number of errros encountered while reading the database file.

warnings Number of warnings encountered while reading the database file.

entries Number of successfully added entries.

locationFile6 Currently loaded location database file.

format6 Location file format

custom6 Number of configured custom locations.

static6 Number of configured locations in the database file (static locations).

lines6 Number of lines in the databse files

errors6 Number of errros encountered while reading the database file.

warnings6 Number of warnings encountered while reading the database file.

entries6 Number of successfully added entries.

flags Information needed for display. This argument passes information from the kernel to the user space.

status This argument displays when the status (success or failure) of database loading.

DatabaseMode This argument displays the database mode.

flushing This argument displays the state of flushing.

loading This argument displays the state of loading.

matchWildcardtoany Indicates whether wildcard qualifiers should match any other qualifier including non-wildcard while evaluating location based expressions. Possible values: Yes, No, Expression. Yes - Wildcard qualifiers match any other qualifiers. No - Wildcard qualifiers do not match non-wildcard qualifiers, but match other wildcard qualifiers. Expression - Wildcard qualifiers in an expression match any qualifier in an LDNS location, wildcard qualifiers in the LDNS location do not match non-wildcard qualifiers in an expression

builtin feature The feature to be checked while applying this config

Example

show locationparameter

nstrace

The following operations can be performed on "nstrace":

show| stop| dump| start|

show nstrace

Display nstrace parameters set through 'start nstrace' command.

Synopsis

show nstrace

Arguments

Output

state Current running state of trace.

scope Scope of started trace, local or cluster level.

traceLocation Directory where current trace files are saved.

nf Number of files to be generated in cycle.

time Time per file (sec).

size Size of the captured data. Set 0 for full packet trace.

mode Capturing mode for trace. Mode can be any of the following values or combination of these values: RX Received packets before NIC pipelining (Filter does not work when RX capturing mode is ON) NEW_RX Received packets after NIC pipelining TX Transmitted packets TXB Packets buffered for transmission IPV6 Translated IPv6 packets C2C Capture C2C message NS_FR_TX TX/TXB packets are not captured in flow receiver. MPTCP MPTCP master flow HTTP_QUIC HTTP-over-QUIC stream data and stream events Default mode: NEW_RX TXB

traceformat Format in which trace will be generated

perNIC Use separate trace files for each interface. Works only with cap format.

fileName Name of the trace file.

fileId ID for the trace file name for uniqueness. Should be used only with -name option.

filter Filter expression for nstrace. Maximum length of filter is 255 and it can be of following format: <expression>

```
&lt;relop> = ( && | || )



&lt;expression> =:

CONNECTION.&lt;qualifier>.&lt;qualifier-method>.(&lt;qualifier-value>)



&lt;qualifier> = SRCIP
```

```
&lt;qualifier-method> = [ EQ | NE ]

&lt;qualifier-value>  = A valid IPv4 address.

example = CONNECTION.SRCIP.EQ(127.0.0.1)



&lt;qualifier> = DSTIP

&lt;qualifier-method> = [ EQ | NE ]

&lt;qualifier-value>  = A valid IPv4 address.

example = CONNECTION.DSTIP.EQ(127.0.0.1)



&lt;qualifier> = IP

&lt;qualifier-method> = [ EQ | NE ]

&lt;qualifier-value>  = A valid IPv4 address.

example = CONNECTION.IP.EQ(127.0.0.1)



&lt;qualifier> = SRCIPv6

&lt;qualifier-method> = [ EQ | NE ]

&lt;qualifier-value>  = A valid IPv6 address.

example = CONNECTION.SRCIPv6.EQ(2001:db8:0:0:1::1)



&lt;qualifier> = DSTIPv6

&lt;qualifier-method> = [ EQ | NE ]

&lt;qualifier-value>  = A valid IPv6 address.
```

```
example = CONNECTION.DSTIPv6.EQ(2001:db8:0:0:1::1)



&lt;qualifier> = IPv6

&lt;qualifier-method> = [ EQ | NE ]

&lt;qualifier-value>  = A valid IPv6 address.

example = CONNECTION.IPv6.EQ(2001:db8:0:0:1::1)



&lt;qualifier> = SRCPORT

&lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE

                    | BETWEEN ]

&lt;qualifier-value>  = A valid port number.

example = CONNECTION.SRCPORT.EQ(80)



&lt;qualifier> = DSTPORT

&lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE

                    | BETWEEN ]

&lt;qualifier-value>  = A valid port number.

example = CONNECTION.DSTPORT.EQ(80)



&lt;qualifier> = PORT

&lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE

                    | BETWEEN ]
```

```
&lt;qualifier-value>  = A valid port number.

example = CONNECTION.PORT.EQ(80)



&lt;qualifier> = VLANID

&lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE

                    | BETWEEN ]

&lt;qualifier-value>  = A valid VLAN ID.

example = CONNECTION.VLANID.EQ(0)



&lt;qualifier> = CONNID

&lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE

                    | BETWEEN ]

&lt;qualifier-value>  = A valid PCB dev number.

example = CONNECTION.CONNID.EQ(0)



&lt;qualifier> = PPEID

&lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE

                    | BETWEEN ]

&lt;qualifier-value>  = A valid core ID.

  example = CONNECTION.PPEID.EQ(0)



&lt;qualifier> = SVCNAME
```

```
&lt;qualifier-method> = [ EQ | NE | CONTAINS | STARTSWITH
                    | ENDSWITH ]
&lt;qualifier-value>  = A valid text string.
example = CONNECTION.SVCNAME.EQ("name")


&lt;qualifier> = LB_VSERVER.NAME
&lt;qualifier-method> = [ EQ | NE | CONTAINS | STARTSWITH
                   | ENDSWITH ]
&lt;qualifier-value>  = LB vserver name.
example = CONNECTION.LB_VSERVER.NAME.EQ("name")


&lt;qualifier> = CS_VSERVER.NAME
&lt;qualifier-method> = [ EQ | NE | CONTAINS | STARTSWITH
                   | ENDSWITH ]
&lt;qualifier-value>  = CS vserver name.
example = CONNECTION.CS_VSERVER.NAME.EQ("name")


&lt;qualifier> = INTF
&lt;qualifier-method> = [ EQ | NE ]
&lt;qualifier-value>  =  A valid interface id in the
               form of x/y.
example = CONNECTION.INTF.EQ("x/y")
```

```
 &lt;qualifier> = SERVICE_TYPE

 &lt;qualifier-method> = [ EQ | NE ]

 &lt;qualifier-value>  = ( SVC_HTTP | FTP | TCP | UDP | SSL |

    SSL_BRIDGE | SSL_TCP | NNTP | RPCSVR | RPCSVRS |

    RPCCLNT | SVC_DNS | ADNS | SNMP | RTSP | DHCPRA | ANY|

    MONITOR | MONITOR_UDP | MONITOR_PING | SIP_UDP |

    SVC_MYSQL | SVC_MSSQL | FIX | SSL_FIX | PKTSTEER |

    SVC_AAA | SERVICE_UNKNOWN )

 example = CONNECTION.SERVICE_TYPE.EQ(ANY)



 &lt;qualifier> = TRAFFIC_DOMAIN_ID

 &lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE

                     | BETWEEN ]

 &lt;qualifier-value>  = A valid traffic domain ID.

 example = CONNECTION.TRAFFIC_DOMAIN_ID.EQ(0)



 eg: start nstrace -filter "CONNECTION.SRCIP.EQ(127.0.0.1) ||
(CONNECTION.SVCNAME.NE("s1") && CONNECTION.SRCPORT.EQ(80))"

 The filter expression should be given in double quotes.
```

common use cases:

Trace capturing full sized traffic from/to ip 10.102.44.111, excluding loopback traffic start nstrace -size 0 -filter "CONNECTION.IP.NE(127.0.0.1) && CONNECTION.IP.EQ(10.102.44.111)"

Trace capturing all traffic to (terminating at) port 80 or 443 start nstrace -size 0 -filter "CONNECTION.DSTPORT.EQ(443) || CONNECTION.DSTPORT.EQ(80)"

Trace capturing all backend traffic specific to service service1 along with corresponding client side traffic start nstrace -size 0 -filter "CONNECTION.SVCNAME.EQ("service1")" -link ENABLED

Trace capturing all traffic through Citrix ADC interface 1/1 start nstrace -filter "CONNECTION.INTF.EQ("1/1")"

Trace capturing all traffic specific through vlan 2 start nstrace -filter "CONNECTION.VLANID.EQ(2)"

Trace capturing all frontend (client side) traffic specific to lb vserver vserver1 along with corresponding server side traffic start nstrace -size 0 -filter "CONNECTION.LB_VSERVER.NAME.EQ("vserver1")" -link ENABLED

link Includes filtered connection's peer traffic.

nodes Nodes on which tracing is started.

merge Specify how traces across PE's are merged

doruntimecleanup Enable or disable runtime temp file cleanup

traceBuffers Number of 16KB trace buffers

skipRPC skip RPC packets

skipLocalSSH skip local SSH packets

capsslkeys Capture SSL Master keys. Master keys will not be captured on FIPS machine. Warning: The captured keys can be used to decrypt information that may be confidential. The captured key files have to be stored in a secure environment

capdroppkt Captures Dropped Packets if set to ENABLED.

inMemoryTrace Logs packets in appliance's memory and dumps the trace file on stopping the nstrace operation

Example

show nstrace

stop nstrace

Stop running Citrix ADC packet capture tool.

Synopsis

stop nstrace

Example

stop nstrace

dump nstrace

dump records from trace buffers to file.

Synopsis

dump nstrace -fileName <string>

Arguments

fileName Name of the trace file.

Example

dump nstrace

start nstrace

Start Citrix ADC packet capture tool. There should be at least 2 GB of free disk space for trace to start

Synopsis

start nstrace

Arguments

nf Number of files to be generated in cycle. Default value: 24 Minimum value: 1 Maximum value: 100

time Time per file (sec). Default value: 3600 Minimum value: 1

size Size of the captured data. Set 0 for full packet trace. Default value: 164 Minimum value: 0 Maximum value: 1514

mode Capturing mode for trace. Mode can be any of the following values or combination of these values: RX Received packets before NIC pipelining (Filter does not work when RX capturing mode is ON) NEW_RX Received packets after NIC pipelining TX Transmitted packets TXB Packets buffered for transmission IPV6 Translated IPv6 packets C2C Capture C2C message NS_FR_TX TX/TXB packets are not captured in flow receiver. MPTCP MPTCP master flow HTTP_QUIC HTTP-over-QUIC stream data and stream events Default mode: NEW_RX TXB Default value: DEFAULT_MODE

perNIC Use separate trace files for each interface. Works only with cap format.

Possible values: ENABLED, DISABLED Default value: DISABLED

fileName Name of the trace file.

fileId ID for the trace file name for uniqueness. Should be used only with -name option.

filter Filter expression for nstrace. Maximum length of filter is 255 and it can be of following format: <expression>

```
&lt;relop> = ( && | || )



&lt;expression> =:

CONNECTION.&lt;qualifier>.&lt;qualifier-method>.(&lt;qualifier-value>)



&lt;qualifier> = SRCIP

&lt;qualifier-method> = [ EQ | NE ]

&lt;qualifier-value>  = A valid IPv4 address.

example = CONNECTION.SRCIP.EQ(127.0.0.1)



&lt;qualifier> = DSTIP

&lt;qualifier-method> = [ EQ | NE ]
```

```
&lt;qualifier-value&gt;  = A valid IPv4 address.

example = CONNECTION.DSTIP.EQ(127.0.0.1)



&lt;qualifier&gt; = IP

&lt;qualifier-method&gt; = [ EQ | NE ]

&lt;qualifier-value&gt;  = A valid IPv4 address.

example = CONNECTION.IP.EQ(127.0.0.1)



&lt;qualifier&gt; = SRCIPv6

&lt;qualifier-method&gt; = [ EQ | NE ]

&lt;qualifier-value&gt;  = A valid IPv6 address.

example = CONNECTION.SRCIPv6.EQ(2001:db8:0:0:1::1)



&lt;qualifier&gt; = DSTIPv6

&lt;qualifier-method&gt; = [ EQ | NE ]

&lt;qualifier-value&gt;  = A valid IPv6 address.

example = CONNECTION.DSTIPv6.EQ(2001:db8:0:0:1::1)



&lt;qualifier&gt; = IPv6

&lt;qualifier-method&gt; = [ EQ | NE ]

&lt;qualifier-value&gt;  = A valid IPv6 address.

example = CONNECTION.IPv6.EQ(2001:db8:0:0:1::1)
```

```
&lt;qualifier> = SRCPORT

&lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE

                    | BETWEEN ]

&lt;qualifier-value>  = A valid port number.

example = CONNECTION.SRCPORT.EQ(80)



&lt;qualifier> = DSTPORT

&lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE

                    | BETWEEN ]

&lt;qualifier-value>  = A valid port number.

example = CONNECTION.DSTPORT.EQ(80)



&lt;qualifier> = PORT

&lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE

                    | BETWEEN ]

&lt;qualifier-value>  = A valid port number.

example = CONNECTION.PORT.EQ(80)



&lt;qualifier> = VLANID

&lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE

                    | BETWEEN ]
```

```
&lt;qualifier-value&gt;  = A valid VLAN ID.

example = CONNECTION.VLANID.EQ(0)



&lt;qualifier&gt; = CONNID

&lt;qualifier-method&gt; = [ EQ | NE | GT | GE | LT | LE

                    | BETWEEN ]

&lt;qualifier-value&gt;  = A valid PCB dev number.

example = CONNECTION.CONNID.EQ(0)



&lt;qualifier&gt; = PPEID

&lt;qualifier-method&gt; = [ EQ | NE | GT | GE | LT | LE

                    | BETWEEN ]

&lt;qualifier-value&gt;  = A valid core ID.

  example = CONNECTION.PPEID.EQ(0)



&lt;qualifier&gt; = SVCNAME

&lt;qualifier-method&gt; = [ EQ | NE | CONTAINS | STARTSWITH

                    | ENDSWITH ]

&lt;qualifier-value&gt;  = A valid text string.

example = CONNECTION.SVCNAME.EQ("name")



&lt;qualifier&gt; = LB_VSERVER.NAME
```

```
&lt;qualifier-method> = [ EQ | NE | CONTAINS | STARTSWITH
                    | ENDSWITH ]
&lt;qualifier-value>  = LB vserver name.
example = CONNECTION.LB_VSERVER.NAME.EQ("name")


&lt;qualifier> = CS_VSERVER.NAME
&lt;qualifier-method> = [ EQ | NE | CONTAINS | STARTSWITH
                    | ENDSWITH ]
&lt;qualifier-value>  = CS vserver name.
example = CONNECTION.CS_VSERVER.NAME.EQ("name")


&lt;qualifier> = INTF
&lt;qualifier-method> = [ EQ | NE ]
&lt;qualifier-value>  =  A valid interface id in the
                form of x/y.
example = CONNECTION.INTF.EQ("x/y")


&lt;qualifier> = SERVICE_TYPE
&lt;qualifier-method> = [ EQ | NE ]
&lt;qualifier-value>  = ( SVC_HTTP | FTP | TCP | UDP | SSL |
   SSL_BRIDGE | SSL_TCP | NNTP | RPCSVR | RPCSVRS |
   RPCCLNT | SVC_DNS | ADNS | SNMP | RTSP | DHCPRA | ANY|
```

```
    MONITOR | MONITOR_UDP | MONITOR_PING | SIP_UDP |

    SVC_MYSQL | SVC_MSSQL | FIX | SSL_FIX | PKTSTEER |

    SVC_AAA | SERVICE_UNKNOWN )

 example = CONNECTION.SERVICE_TYPE.EQ(ANY)



 &lt;qualifier> = TRAFFIC_DOMAIN_ID

 &lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE

                     | BETWEEN ]

 &lt;qualifier-value>  = A valid traffic domain ID.

 example = CONNECTION.TRAFFIC_DOMAIN_ID.EQ(0)



 eg: start nstrace -filter "CONNECTION.SRCIP.EQ(127.0.0.1) ||
(CONNECTION.SVCNAME.NE("s1") && CONNECTION.SRCPORT.EQ(80))"

 The filter expression should be given in double quotes.
```

common use cases:

Trace capturing full sized traffic from/to ip 10.102.44.111, excluding loopback traffic start nstrace -size 0 -filter "CONNECTION.IP.NE(127.0.0.1) && CONNECTION.IP.EQ(10.102.44.111)"

Trace capturing all traffic to (terminating at) port 80 or 443 start nstrace -size 0 -filter "CONNECTION.DSTPORT.EQ(443) || CONNECTION.DSTPORT.EQ(80)"

Trace capturing all backend traffic specific to service service1 along with corresponding client side traffic start nstrace -size 0 -filter "CONNECTION.SVCNAME.EQ("service1")" -link ENABLED

Trace capturing all traffic through Citrix ADC interface 1/1 start nstrace -filter "CONNECTION.INTF.EQ("1/1")"

Trace capturing all traffic specific through vlan 2 start nstrace -filter "CONNECTION.VLANID.EQ(2)"

Trace capturing all frontend (client side) traffic specific to lb vserver vserver1 along with corresponding server side traffic start nstrace -size 0 -filter "CONNECTION.LB_VSERVER.NAME.EQ("vserver1")" -link ENABLED

link Includes filtered connection's peer traffic.

Possible values: ENABLED, DISABLED Default value: DISABLED

nodes Nodes on which tracing is started.

Minimum value: 0 Maximum value: 32

filesize File size, in MB, treshold for rollover. If free disk space is less than 2GB at the time of rollover, trace will stop

Default value: 1024 Minimum value: 0 Maximum value: 10240

traceformat Format in which trace will be generated

Possible values: NSCAP, PCAP Default value: 0

merge Specify how traces across PE's are merged

Possible values: ONSTOP, ONTHEFLY, NOMERGE Default value: 0

doruntimecleanup Enable or disable runtime temp file cleanup

Possible values: ENABLED, DISABLED Default value: ENABLED

traceBuffers Number of 16KB trace buffers Default value: 5000 Minimum value: 1000

skipRPC skip RPC packets

Possible values: ENABLED, DISABLED Default value: DISABLED

skipLocalSSH skip local SSH packets

Possible values: ENABLED, DISABLED Default value: DISABLED

capsslkeys Capture SSL Master keys. Master keys will not be captured on FIPS machine. Warning: The captured keys can be used to decrypt information that may be confidential. The captured key files have to be stored in a secure environment

Possible values: ENABLED, DISABLED Default value: DISABLED

capdroppkt Captures Dropped Packets if set to ENABLED.

Possible values: ENABLED, DISABLED Default value: DISABLED

inMemoryTrace Logs packets in appliance's memory and dumps the trace file on stopping the nstrace operation

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

start nstrace -time 10

radiusNode

The following operations can be performed on "radiusNode":

add| show| set| rm|

add radiusNode

add a radiusnode and its secret key configuration on NS

Synopsis

add radiusNode <nodePrefix> -radKey

Arguments

nodePrefix IP address/IP prefix of radius node in CIDR format

radKey The key shared between the RADIUS server and clients. Required for Citrix ADC to communicate with the RADIUS nodes.

Example

add radiusnode 10.102.10.0/8 -radkey secret_key1

show radiusNode

show radius node configuration

Synopsis

show radiusNode

Arguments

nodePrefix IP address/IP prefix of radius node in CIDR format

Output

radKey The key shared between the RADIUS server and clients. Required for Citrix ADC to communicate with the RADIUS nodes.

stateflag To maintain state

devno count

Example

show radius node 10.102.10.0/8

set radiusNode

set secret key configuration of radius node

Synopsis

set radiusNode <nodePrefix> -radKey

Arguments

nodePrefix IP address/IP prefix of radius node in CIDR format

radKey The key shared between the RADIUS server and clients. Required for Citrix ADC to communicate with the RADIUS nodes.

Example

set radiusnode 10.102.10.0/8 -radkey secret_key2

rm radiusNode

remove radius node configuration from NS

Synopsis

rm radiusNode <nodePrefix>

Arguments

nodePrefix IP address/IP prefix of radius node in CIDR format

Example

rm radiusnode 10.102.10.0/8

reporting

The following operations can be performed on "reporting":

show| enable| disable|

show reporting

show the state of data collection for reporting module.

Synopsis

show reporting

Arguments

Output

state The rule associated with the entity

Example

show reporting

enable reporting

Enable the data collection for reporting module.

Synopsis

enable reporting

Example

enable reporting

disable reporting

Disable the data collection for reporting module.

Synopsis

disable reporting

Example

disable reporting

reportingconfig

The following operations can be performed on "reportingconfig":

rm| add| show|

rm reportingconfig

This api removes the entity configured for flexible monitoring/reporting

Synopsis

rm reportingconfig <EntityTypes>

Arguments

EntityTypes Object type of the entity

Possible values: appfwpolicy, appfwpolicylabel, appfwprofile, appqoepolicy, authenticationloginschemapolicy, authenticationoauthidppolicy, authenticationpolicy, authenticationpolicylabel, authenticationsamlidppolicy, authenticationvserver, authorizationpolicylabel, botpolicy, botpolicylabel, botprofile, cachecontentgroup, cachepolicy, cachepolicylabel, cmppolicy, cmppolicylabel, contentinspectionpolicy, contentinspectionpolicylabel, crvserver, csvserver, dnspolicylabel, dnsrecords, dospolicy, gslbdomain, gslbservice, gslbservicegroup, gslbservicegroupmember, gslbsite, gslbvserver, inat, inatsession, lbvserver, lldp, nsacl, nsacl6, nslimitidentifier, nsmemory, nspbr, nspbr6, pcpserver, responderpolicy, responderpolicylabel, rewritepolicy, rewritepolicylabel, rnatip, service, servicegroup, servicegroupmember, spilloverpolicy, sslvserver, tmsessionpolicy, tmtrafficpolicy, tunnelip, tunnelip6, uservserver, videooptimizationdetectionpolicy, videooptimizationdetectionpolicylabel, videooptimizationpacingpolicy, videooptimizationpacingpolicylabel, vlan, vxlan

name Name of the entity

add reportingconfig

This api adds the entity configured for flexible monitoring/reporting

Synopsis

add reportingconfig <EntityTypes>

Arguments

EntityTypes Object type of the entity

Possible values: appfwpolicy, appfwpolicylabel, appfwprofile, appqoepolicy, authenticationloginschemapolicy, authenticationoauthidppolicy, authenticationpolicy, authenticationpolicylabel, authenticationsamlidppolicy, authenticationvserver, authorizationpolicylabel, botpolicy, botpolicylabel, botprofile, cachecontentgroup, cachepolicy, cachepolicylabel, cmppolicy, cmppolicylabel, contentinspectionpolicy, contentinspectionpolicylabel, crvserver, csvserver, dnspolicylabel, dnsrecords, dospolicy, gslbdomain, gslbservice, gslbservicegroup, gslbservicegroupmember, gslbsite, gslbvserver, inat, inatsession, lbvserver, lldp, nsacl, nsacl6, nslimitidentifier, nsmemory, nspbr, nspbr6, pcpserver, responderpolicy, responderpolicylabel, rewritepolicy, rewritepolicylabel, rnatip, service, servicegroup, servicegroupmember, spilloverpolicy, sslvserver, tmsessionpolicy, tmtrafficpolicy, tunnelip, tunnelip6, uservserver, videooptimizationdetectionpolicy, videooptimizationdetectionpolicylabel, videooptimizationpacingpolicy, videooptimizationpacingpolicylabel, vlan, vxlan

name Name of the entity

show reportingconfig

This api displays the entity configured for flexible monitoring/reporting

Synopsis

show reportingconfig

Arguments

EntityTypes object type of the entity

Possible values: appfwpolicy, appfwpolicylabel, appfwprofile, appqoepolicy, authenticationloginschemapolicy, authenticationoauthidppolicy, authenticationpolicy, authenticationpolicylabel, authenticationsamlidppolicy, authenticationvserver, authorizationpolicylabel, botpolicy, botpolicylabel, botprofile, cachecontentgroup, cachepolicy, cachepolicylabel, cmppolicy, cmppolicylabel, contentinspectionpolicy, contentinspectionpolicylabel, crvserver, csvserver, dnspolicylabel, dnsrecords, dospolicy, gslbdomain, gslbservice, gslbservicegroup, gslbservicegroupmember, gslbsite, gslbvserver, inat, inatsession, lbvserver, lldp, nsacl, nsacl6, nslimitidentifier, nsmemory, nspbr, nspbr6, pcpserver, responderpolicy, responderpolicylabel, rewritepolicy, rewritepolicylabel, rnatip, service, servicegroup, servicegroupmember, spilloverpolicy, sslvserver, tmsessionpolicy, tmtrafficpolicy, tunnelip,

tunnelip6, uservserver, videooptimizationdetectionpolicy, videooptimizationdetectionpolicylabel, videooptimizationpacingpolicy, videooptimizationpacingpolicylabel, vlan, vxlan

name name of the entity

Output

devno count stateflag

server

The following operations can be performed on "server":

disable| rename| set| add| rm| show| unset| enable|

disable server

Disables all services on the server. When a server is disabled, all services on the server are disabled.

Synopsis

disable server <name>@

Arguments

name Name of the server to disable.

delay Time, in seconds, after which all the services configured on the server are disabled.

graceFul Shut down gracefully, without accepting any new connections, and disabling each service when all of its connections are closed.

Possible values: YES, NO Default value: NO

Example

disable server web_svr 30 To disable all the services configured on servers named serv1, serv2 and serv3 at once, use the following command: disable server serv

Related Commands

- disable service

rename server

Renames a server.

Synopsis

rename server <name>@ <newName>@

Arguments

name Existing name of the server.

newName New name for the server. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

Example

rename server s1 s1-new

set server

Modifies the specified parameters of a server entry.

Synopsis

set server <name>@

Arguments

name Name of the server whose parameters you are configuring.

IPAddress Name of the server whose parameters you are configuring.

domainResolveRetry Time, in seconds, for which the Citrix ADC must wait, after DNS resolution fails, before sending the next DNS query to resolve the domain name. Default value: 5 Minimum value: 5 Maximum value: 20939

translationIp IP address used to transform the server's DNS-resolved IP address.

translationMask The netmask of the translation ip

domainResolveNow Immediately send a DNS query to resolve the server's domain name.

comment Any information about the server.

Example

set server http_svr -IPAddress 10.102.1.112 To set multiple servers IP addresses at once you can use the following command: setserver serv -IPAddress 10.102.27. The above command sets the IP address of serv1 to 10.102.27.1, serv2 to 10.102.27.2 and serv3 to 10.102.27.3.

add server

Creates a server entry on the Citrix ADC. The Citrix ADC appliance supports two types of servers: IP address based servers and domain based servers.

Synopsis

add server <name>@ (<IPAddress>@ | (<domain>@) | (-translationIp <ip_addr> -translationMask <netmask>))

Arguments

name Name for the server. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the name is created.

IPAddress IPv4 or IPv6 address of the server. If you create an IP address based server, you can specify the name of the server, instead of its IP address, when creating a service. Note: If you do not create a server entry, the server IP address that you enter when you create a service becomes the name of the server.

domain Domain name of the server. For a domain based configuration, you must create the server first.

translationIp IP address used to transform the server's DNS-resolved IP address.

translationMask The netmask of the translation ip

domainResolveRetry Time, in seconds, for which the Citrix ADC must wait, after DNS resolution fails, before sending the next DNS query to resolve the domain name. Default value: 5 Minimum value: 5 Maximum value: 20939

state Initial state of the server.

Possible values: ENABLED, DISABLED Default value: ENABLED

IPv6Address Support IPv6 addressing mode. If you configure a server with the IPv6 addressing mode, you cannot use the server in the IPv4 addressing mode.

Possible values: YES, NO Default value: NO

comment Any information about the server.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

queryType Specify the type of DNS resolution to be done on the configured domain to get the backend services. Valid query types are A, AAAA and SRV with A being the default querytype. The type of DNS resolution done on the domains in SRV records is inherited from ipv6 argument.

Possible values: A, AAAA, SRV Default value: A

Example

add server web_serv 10.102.27.150 To add multiple servers you can use the following command: add server serv 10.102.27. The above command adds three servers: serv1 with IP 10.102.27.151, serv2 with IP 10.102.27.152 and serv3 with IP 10.102.27.153.

Related Commands

- add service

rm server

Removes a server entry from the Citrix ADC.

Synopsis

rm server <name>@ ...

Arguments

name Name of the server entry to remove.

Example

rm server web_svr To remove the servers named serv1, serv2 and serv3 at once you can use the following command: rm server serv

Related Commands

- rm service

show server

Displays the parameters of all the server entries on the appliance, or the parameters of the specified server entry.

Synopsis

show server

Arguments

name Name of the server for which to display parameters.

internal Display names of the servers that have been created for internal use.

Output

IPAddress The IP Address of server.

state The State of the server.

domain The domain name of the server.

domainResolveRetry Time, in seconds, for which the Citrix ADC must wait, after DNS resolution fails, before sending the next DNS query to resolve the domain name.

serviceName The services attatched to the server.

serviceGroupName servicegroups bind to this server

translationIp IP address used to transform the server's DNS-resolved IP address.

translationMask The netmask of the translation ip

comment Any information about the server.

stateflag stateflag

serviceType The type of bound service

serviceIPAddress The IP address of the bound service

serviceIPstr This field has been intorduced to show the dbs services ip

port The port number to be used for the bound service.

svrState The state of the bound service

stateChangeTimeSec Time when last state change happened. Seconds part.

ticksSinceLastStateChange Time in 10 millisecond ticks since the last state change.

IPv6Address Support IPv6 addressing mode. If you configure a server with the IPv6 addressing mode, you cannot use the server in the IPv4 addressing mode.

svrcfgFlags Contains config info about the service like LOOPBACK/DMNBASED/INTERNAL

port port of the service.

serviceType service type of the service.

svrcfgFlags service flags to denote its a db enabled.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

autoScale Auto scale option for a servicegroup

CustomServerID A positive integer to identify the service. Used when the persistency type is set to Custom Server ID.

monThreshold Minimum sum of weights of the monitors that are bound to this service. Used to determine whether to mark a service as UP or DOWN.

maxClient Maximum number of simultaneous open connections for the service group.

maxReq Maximum number of requests that can be sent on a persistent connection to the service group. Note: Connection requests beyond this value are rejected.

maxBandwidth Maximum bandwidth, in Kbps, allocated for all the services in the service group.

usip Use the client's IP address as the source IP address when initiating a connection to the server. When creating a service, if you do not set this parameter, the service inherits the global Use Source IP setting (available in the enable ns mode and disable ns mode CLI commands, or in the System > Settings > Configure modes > Configure Modes dialog box). However, you can override this setting after you create the service.

CKA Enable client keep-alive for the service group.

TCPB Enable TCP buffering for the service group.

CMP Enable compression for the specified service.

cltTimeout Time, in seconds, after which to terminate an idle client connection.

svrTimeout Time, in seconds, after which to terminate an idle server connection.

cipHeader Name of the HTTP header whose value must be set to the IP address of the client. Used with the Client IP parameter. If client IP insertion is enabled, and the client IP header is not specified, the value of Client IP Header parameter or the value set by the set ns config command is used as client's IP header name.

cip Before forwarding a request to the service, insert an HTTP header with the client's IPv4 or IPv6 address as its value. Used if the server needs the client's IP address for security, accounting, or other purposes, and setting the Use Source IP parameter is not a viable option.

cacheable Use the transparent cache redirection virtual server to forward the request to the cache server.

sp Enable surge protection for the service group.

downStateFlush Perform delayed clean-up of connections to all services in the service group.

appflowLog Enable logging of AppFlow information for the specified service group.

boundTD Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

queryType Specify the type of DNS resolution to be done on the configured domain to get the backend services. Valid query types are A, AAAA and SRV with A being the default querytype. The type of DNS resolution done on the domains in SRV records is inherited from ipv6 argument.

serviceGroupEntName2 Used for show server of SRV type to indicate target FQDNs

svcitmPriority Indicates the Priority of the SRV target FQDN

svcitmActSvcs Indicates the total number of active IPs for SRV target FQDN

svcitmBoundSvcs Indicates the total number of bound IPs for the SRV target FQDN

weight Indicates the weight of bound IPs

devno count

Example

> show server web_svr1 Name: web_svr1 State:ENABLED IPAddress: 10.102.27.154

> show server web_svr1 Name: web_svr2 State:ENABLED Domain: <www.abc.com> Resolve Retry: 30 Secs Translation IP: 10.102.27.153 Translation Mask: 255.255.255.0

Related Commands

- show service

unset server

Use this command to remove server settings.Refer to the set server command for meanings of the arguments.

Synopsis

unset server <name>@ -comment

enable server

Enables all services on the specified server.

Synopsis

enable server <name>@

Arguments

name Name of the server to enable.

Example

enable server web_serv To enable all the services configured on servers named serv1, serv2 and serv3 at once, use the following command: enable server serv

Related Commands

- enable service

service

The following operations can be performed on "service":

rename| unbind| enable| stat| rm| disable| set| add| unset| show| bind|

rename service

Renames a service.

Synopsis

rename service <name>@ <newName>@

Arguments

name Existing name of the service to be renamed.

newName New name for the service. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

Example

rename service svc1 svcnew

unbind service

Unbinds a monitor from the specified service.

Synopsis

unbind service <name>@

Arguments

name Name of the service from which to unbind a monitor.

monitorName Name of the monitor assigned to the service.

Example

unbind service http_svc -monitorName mon1 To unbind a monitor called mon1 on services svc1, svc2 and svc3, use the following command: unbind service svc -monitorName mon1

enable service

Enables a service.

Synopsis

enable service <name>@

Arguments

name Name of the service.

Example

enable service http_svc To enable svc1, svc2 and svc3 in one go use the following command: enable service svc

Related Commands

- enable vserver

stat service

Displays statistics that have been collected for the specified service.

Synopsis

stat service

Arguments

name Name of the service.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Throughput (Mbps) (Throughput) Number of bytes received or sent by this service (Mbps).

Average server TTFB (SvrTTFB) Average TTFB between the Citrix ADC and the server. TTFB is the time interval between sending the request packet to a service and receiving the first response from the service

Number of Bytes processed by ADS Service Total IP payload sent and received

IP address (IP) The IP address on which the service is running.

Port (port) The port on which the service is running.

Service type (Type) The service type of this service.Possible values are ADNS, DNS, MYSQL, RTSP, SSL_DIAMETER, ADNS_TCP, DNS_TCP, NNTP, SIP_UDP, SSL_TCP, ANY, FTP, RADIUS, SNMP, TCP, DHCPRA, HTTP, RDP, SSL, TFTP, DIAMETER, MSSQL, RPCSVR, SSL_BRIDGE, UDP

State Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)

Requests (Req) Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Responses (Rsp) Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Request bytes (Reqb) Total number of request bytes received on this service or virtual server.

Response bytes (Rspb) Number of response bytes received by this service or virtual server.

Current client connections (ClntConn) Number of current client connections.

Requests in surge queue (SurgeQ) Number of requests in the surge queue.

Current server connections (SvrConn) Number of current connections to the actual servers behind the virtual server.

Current Server Est connections (SvrEstConn) Number of server connections in ESTABLISHED state.

Connections in reuse pool (ReuseP) Number of requests in the idle queue/reuse pool.

Maximum server connections (MaxConn) Maximum open connections allowed on this service.

Current load on the service (Load) Load on the service that is calculated from the bound load based monitor.

No of TCPConn ReasmQ 75% reached (ReassQ75) Total no of connections with 75% TCP reassembly queue

No of TCPConn ReasmQ Flushed (ReassQFlush) Total no of connections incurred TCP reassembly queue flush

Failed to respond to request (AddedSkipListCount) Number of times this service/servicegroup failed to respond to a request,triggering retry to other service.

No of http max header size packet parsing failures (httpMaxHdrSzPkts) Number of http max header size packet parsing failures

Number of HTTP requests exceeding max header field length (httpMaxHdrFldLenPkts) Number of HTTP requests exceeding max header field length

max ooo packets threshold hits (tcpMaxoooPkts) No of times max out of order packets reached

Current flags on the service (CurtFlags) Current flags on the service for internal use in display handlers.

Total transactions for server TTLB (totSvrTTLBTransactions) Total transactions where server TTLB is calculated.

Tolerating TTLB Transactions (toleratingTTLBTransactions) Tolerable transactions based on APDEX threshold (>T && <4T).

Frustrating TTLB Transactions (frustratingTTLBTransactions) Frustrating transactions based on APDEX threshold (>4T).

Service hits (Hits) Number of times that the service has been provided.

ActvTrans Number of active transactions handled by this service. (Including those in the surge queue.) Active Transaction means number of transactions currently served by the server including those waiting in the SurgeQ

Binding Order (Order) Order with which service is bound to vserver

Total Packets rcvd (PktRx) Total number of packets received by this service or virtual server.

Total Packets sent (PktTx) Total number of packets sent.

Related Commands

- stat serviceGroupMember

rm service

Removes a service.

Synopsis

rm service <name>@

Arguments

name Name of the service.

Example

rm service http_svc To remove services svc1, svc2 and svc3 in one go use the following command: rm service svc

disable service

Disables a service.

Synopsis

disable service <name>@

Arguments

name Name of the service.

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

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

Possible values: YES, NO Default value: NO

Example

disable service http_svc 10 To disable svc1, svc2 and svc3 in one go use the following command: disable service svc 10

set service

Modifies the parameters of an existing service.

Synopsis

set service <name>@ [-cip (ENABLED | DISABLED)]

Arguments

name Name of the service for which to modify parameters.

IPAddress The new IP address of the service.

maxClient Maximum number of simultaneous open connections to the service. Minimum value: 0 Maximum value: 4294967294

maxReq Maximum number of requests that can be sent on a persistent connection to the service. Note: Connection requests beyond this value are rejected. Minimum value: 0 Maximum value: 65535

cacheable Use the transparent cache redirection virtual server to forward requests to the cache server. Note: Do not specify this parameter if you set the Cache Type parameter.

Possible values: YES, NO Default value: NO

cip Before forwarding a request to the service, insert an HTTP header with the client's IPv4 or IPv6 address as its value. Used if the server needs the client's IP address for security, accounting, or other purposes, and setting the Use Source IP parameter is not a viable option.

Possible values: ENABLED, DISABLED

cipHeader Name for the HTTP header whose value must be set to the IP address of the client. Used with the Client IP parameter. If you set the Client IP parameter, and you do not specify a name for the header, the appliance uses the header name specified for the global Client IP Header parameter (the cipHeader parameter in the set ns param CLI command or the Client IP Header parameter in the Configure HTTP Parameters dialog box at System > Settings > Change HTTP parameters). If the global Client IP Header parameter is not specified, the appliance inserts a header with the name "client-ip."

usip Use the client's IP address as the source IP address when initiating a connection to the server. When creating a service, if you do not set this parameter, the service inherits the global Use Source IP setting (available in the enable ns mode and disable ns mode CLI commands, or in the System > Settings > Configure modes > Configure Modes dialog box). However, you can override this setting after you create the service.

Possible values: YES, NO

pathMonitor Path monitoring for clustering

Possible values: YES, NO

pathMonitorIndv Individual Path monitoring decisions

Possible values: YES, NO

useproxyport Use the proxy port as the source port when initiating connections with the server. With the NO setting, the client-side connection port is used as the source port for the server-side connection. Note: This parameter is available only when the Use Source IP (USIP) parameter is set to YES.

Possible values: YES, NO

sp Enable surge protection for the service.

Possible values: ON, OFF

rtspSessionidRemap Enable RTSP session ID mapping for the service.

Possible values: ON, OFF Default value: OFF

healthMonitor Monitor the health of this service. Available settings function as follows: YES - Send probes to check the health of the service. NO - Do not send probes to check the health of the service. With the NO option, the appliance shows the service as UP at all times.

Possible values: YES, NO Default value: YES

cltTimeout Time, in seconds, after which to terminate an idle client connection. Maximum value: 31536000

svrTimeout Time, in seconds, after which to terminate an idle server connection. Maximum value: 31536000

CustomServerID Unique identifier for the service. Used when the persistency type for the virtual server is set to Custom Server ID. Default value: "None"

CKA Enable client keep-alive for the service.

Possible values: YES, NO

TCPB Enable TCP buffering for the service.

Possible values: YES, NO

CMP Enable compression for the service.

Possible values: YES, NO

maxBandwidth Maximum bandwidth, in Kbps, allocated to the service. Minimum value: 0 Maximum value: 4294967287

accessDown Use Layer 2 mode to bridge the packets sent to this service if it is marked as DOWN. If the service is DOWN, and this parameter is disabled, the packets are dropped.

Possible values: YES, NO Default value: NO

monThreshold Minimum sum of weights of the monitors that are bound to this service. Used to determine whether to mark a service as UP or DOWN. Minimum value: 0 Maximum value: 65535

weight Weight to assign to the monitor-service binding. When a monitor is UP, the weight assigned to its binding with the service determines how much the monitor contributes toward keeping the health of the service above the value configured for the Monitor Threshold parameter. Minimum value: 1 Maximum value: 100

monitorName Name of the monitor bound to the specified service.

downStateFlush Flush all active transactions associated with a service whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions.

Possible values: ENABLED, DISABLED Default value: ENABLED

tcpProfileName Name of the TCP profile that contains TCP configuration settings for the service.

httpProfileName Name of the HTTP profile that contains HTTP configuration settings for the service.

contentInspectionProfileName Name of the ContentInspection profile that contains IPS/IDS communication related setting for the service

hashId A numerical identifier that can be used by hash based load balancing methods. Must be unique for each service. Minimum value: 1

comment Any information about the service.

appflowLog Enable logging of AppFlow information.

Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile Network profile to use for the service.

processLocal By turning on this option packets destined to a service in a cluster will not under go any steering. Turn this option for single packet request response mode or when the upstream device is performing a proper RSS for connection based distribution.

Possible values: ENABLED, DISABLED Default value: DISABLED

dnsProfileName Name of the DNS profile to be associated with the service. DNS profile properties will applied to the transactions processed by a service. This parameter is valid only for ADNS and ADNS-TCP services.

monConnectionClose Close monitoring connections by sending the service a connection termination message with the specified bit set.

Possible values: RESET, FIN Default value: NONE

Example

set service http_svc -maxClient 100 The following command sets IP address 10.102.27.53 for service svc1, 10.102.27.54 for svc2 and 10.102.27.55 for svc3. set service svc -IPAddress 10.102.27.

add service

Creates a service on the Citrix ADC. If the service is domain based, before you create the service, create the server entry by using the add server command. Then, in this command, specify the Server parameter.

Synopsis

add service <name>@ (<IP>@ | <serverName>@) <serviceType> <port> [-cip (ENABLED | DISABLED)]

Arguments

name Name for the service. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the service has been created.

IP IP to assign to the service.

serverName Name of the server that hosts the service.

serviceType Protocol in which data is exchanged with the service.

Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, ADNS_TCP, MYSQL, MSSQL, ORACLE, MONGO, MONGO_TLS, RADIUS, RADIUSListener, RDP, DIAMETER, SSL_DIAMETER, TFTP, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, LOGSTREAM_SSL, MQTT, MQTT_TLS, QUIC_BRIDGE

port Port number of the service.

clearTextPort Port to which clear text data must be sent after the appliance decrypts incoming SSL traffic. Applicable to transparent SSL services. Minimum value: 1

cacheType Cache type supported by the cache server.

Possible values: TRANSPARENT, REVERSE, FORWARD

maxClient Maximum number of simultaneous open connections to the service. Minimum value: 0 Maximum value: 4294967294

healthMonitor Monitor the health of this service. Available settings function as follows: YES - Send probes to check the health of the service. NO - Do not send probes to check the health of the service. With the NO option, the appliance shows the service as UP at all times.

Possible values: YES, NO Default value: YES

maxReq Maximum number of requests that can be sent on a persistent connection to the service. Note: Connection requests beyond this value are rejected. Minimum value: 0 Maximum value: 65535

cacheable Use the transparent cache redirection virtual server to forward requests to the cache server. Note: Do not specify this parameter if you set the Cache Type parameter.

Possible values: YES, NO Default value: NO

cip Before forwarding a request to the service, insert an HTTP header with the client's IPv4 or IPv6 address as its value. Used if the server needs the client's IP address for security, accounting, or other purposes, and setting the Use Source IP parameter is not a viable option.

Possible values: ENABLED, DISABLED

cipHeader Name for the HTTP header whose value must be set to the IP address of the client. Used with the Client IP parameter. If you set the Client IP parameter, and you do not specify a name for the header, the appliance uses the header name specified for the global Client IP Header parameter (the cipHeader parameter in the set ns param CLI command or the Client IP Header parameter in the Configure HTTP Parameters dialog box at System > Settings > Change HTTP parameters). If the global Client IP Header parameter is not specified, the appliance inserts a header with the name "client-ip."

usip Use the client's IP address as the source IP address when initiating a connection to the server. When creating a service, if you do not set this parameter, the service inherits the global Use Source IP setting (available in the enable ns mode and disable ns mode CLI commands, or in the System > Settings > Configure modes > Configure Modes dialog box). However, you can override this setting after you create the service.

Possible values: YES, NO

pathMonitor Path monitoring for clustering

Possible values: YES, NO

pathMonitorIndv Individual Path monitoring decisions

Possible values: YES, NO

useproxyport Use the proxy port as the source port when initiating connections with the server. With the NO setting, the client-side connection port is used as the source port for the server-side connection. Note: This parameter is available only when the Use Source IP (USIP) parameter is set to YES.

Possible values: YES, NO

sp Enable surge protection for the service.

Possible values: ON, OFF

rtspSessionidRemap Enable RTSP session ID mapping for the service.

Possible values: ON, OFF Default value: OFF

cltTimeout Time, in seconds, after which to terminate an idle client connection. Maximum value: 31536000

svrTimeout Time, in seconds, after which to terminate an idle server connection. Maximum value: 31536000

CustomServerID Unique identifier for the service. Used when the persistency type for the virtual server is set to Custom Server ID. Default value: "None"

CKA Enable client keep-alive for the service.

Possible values: YES, NO

TCPB Enable TCP buffering for the service.

Possible values: YES, NO

CMP Enable compression for the service.

Possible values: YES, NO

maxBandwidth Maximum bandwidth, in Kbps, allocated to the service. Minimum value: 0 Maximum value: 4294967287

accessDown Use Layer 2 mode to bridge the packets sent to this service if it is marked as DOWN. If the service is DOWN, and this parameter is disabled, the packets are dropped.

Possible values: YES, NO Default value: NO

monThreshold Minimum sum of weights of the monitors that are bound to this service. Used to determine whether to mark a service as UP or DOWN. Minimum value: 0 Maximum value: 65535

state Initial state of the service.

Possible values: ENABLED, DISABLED Default value: ENABLED

downStateFlush Flush all active transactions associated with a service whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions.

Possible values: ENABLED, DISABLED Default value: ENABLED

tcpProfileName Name of the TCP profile that contains TCP configuration settings for the service.

httpProfileName Name of the HTTP profile that contains HTTP configuration settings for the service.

contentInspectionProfileName Name of the ContentInspection profile that contains IPS/IDS communication related setting for the service

hashId A numerical identifier that can be used by hash based load balancing methods. Must be unique for each service. Minimum value: 1

comment Any information about the service.

appflowLog Enable logging of AppFlow information.

Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile Network profile to use for the service.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

processLocal By turning on this option packets destined to a service in a cluster will not under go any steering. Turn this option for single packet request response mode or when the upstream device is performing a proper RSS for connection based distribution.

Possible values: ENABLED, DISABLED Default value: DISABLED

dnsProfileName Name of the DNS profile to be associated with the service. DNS profile properties will applied to the transactions processed by a service. This parameter is valid only for ADNS and ADNS-TCP services.

monConnectionClose Close monitoring connections by sending the service a connection termination message with the specified bit set.

Possible values: RESET, FIN Default value: NONE

Example

add service http_svc 10.102.1.112 http 80 The below command adds the service web_svc1 for the server web_serv1, web_svc2 for web_serv2 and web_svc3 for web_serv3. add service web_svc web_serv http 80

unset service

Removes the parameter settings of the specified service. Attributes for which a default value is available revert to their default values..Refer to the set service command for meanings of the arguments.

Synopsis

unset service <name>@

Example

unset service http_svc -maxClient To unset maxclients for services svc1, svc2 and svc3, the following command can be used: unset service svc -maxClient

show service

Displays a list of all services configured on the Citrix ADC, or the configuration details of the specified service.

Synopsis

show service show service bindings - alias for 'show svcbindings'

Arguments

name Name of the service for which to display configuration details.

all Display both user-configured and dynamically learned services.

internal Display only dynamically learned services.

Output

numOfconnections This will tell the number of client side connections are still open.

serverName The name of the server for which a service has created.

policyName The name of the policyname for which this service is bound

serviceType The type of service

serviceConfTpye The configuration type of the service

serviceConfType The configuration type of the service

serviceConfType2 The configuration type of the service (Internal/Dynamic/Configured).

port Port number of the service.

value SSL status.

clearTextPort The clear-text port number where clear-text data is sent. Used with SSL offload service

gslb The GSLB option for the corresponding virtual server.

cacheType Cache type supported by the cache server.

maxClient Maximum number of simultaneous open connections to the service.

maxReq Maximum number of requests that can be sent on a persistent connection to the service. Note: Connection requests beyond this value are rejected.

cacheable Use the transparent cache redirection virtual server to forward requests to the cache server. Note: Do not specify this parameter if you set the Cache Type parameter.

cip Before forwarding a request to the service, insert an HTTP header with the client's IPv4 or IPv6 address as its value. Used if the server needs the client's IP address for security, accounting, or other purposes, and setting the Use Source IP parameter is not a viable option.

cipHeader The client IP header.

usip The use of client's IP Address option.

pathMonitor Path monitoring for clustering

pathMonitorIndv Individual Path monitoring for decisions.

useproxyport The use of client's Port.

weight The weight of the monitor.

state Added this field for getting state value from table.

sp Enable surge protection for the service.

rtspSessionidRemap Enable RTSP session ID mapping for the service.

failedprobes Number of the current failed monitoring probes.

cltTimeout The idle time in seconds after which the client connection is terminated.

totalprobes The total number of probs sent.

svrTimeout The idle time in seconds after which the server connection is terminated.

totalfailedprobes The total number of failed probs.

publicIP public ip

publicPort public port

CustomServerID The identifier for the service. Used when the persistency type is set to Custom Server ID.

serverID The identifier for the service. This is used when the persistency type is set to Custom Server ID.

CKA Enable client keep-alive for the service.

TCPB Enable TCP buffering for the service.

processLocal By turning on this option packets destined to a service in a cluster will not under go any steering. Turn this option for single packet request response mode or when the upstream device is performing a proper RSS for connection based distribution.

CMP Enable compression for the service.

maxBandwidth The maximum bandwidth in kbps allowed for the service

accessDown The option to allow access to disabled or down services. If enabled, all packets to the service are bridged; if disabled, they are dropped.

svrState The state of the service

delay The remaining time in seconds for the service to be disabled

IPAddress The IP address of the server.

monitorName The monitor Names.

monThreshold Minimum sum of weights of the monitors that are bound to this service. Used to determine whether to mark a service as UP or DOWN.

monState The configured state (enable/disable) of the monitor on this server.

monState The running state of the monitor on this service.

monStatCode The code indicating the monitor response.

lastresponse The string form of monstatcode.

responseTime Response time of this monitor.

monStatParam1 First parameter for use with message code.

monStatParam2 Second parameter for use with message code.

monStatParam3 Third parameter for use with message code.

downStateFlush Flush all active transactions associated with a service whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions.

stateChangeTimeSec Time when last state change happened. Seconds part.

stateChangeTimemSec Time at which last state change happened. Milliseconds part.

timeSinceLastStateChange Time in milliseconds since the last state change.

ticksSinceLastStateChange Time in 10 millisecond ticks since the last state change.

StateUpdateReason Checks state update reason on the secondary node.

ClMonOwner Tells the mon owner of the service.

ClMonView Tells the view id of the monitoring owner.

tcpProfileName Name of the TCP profile.

httpProfileName Name of the HTTP profile that contains HTTP configuration settings for the service.

contentInspectionProfileName Name of the ContentInspection profile that contains IPS/IDS communication related setting for the service

hashId A numerical identifier that can be used by hash based load balancing methods. Must be unique for each service.

graceFul Indicates graceful shutdown of the service. System will wait for all outstanding connections to this service to be closed before disabling the service.

comment Comments associated with this service.

monitorTotalProbes Total number of probes sent to monitor this service.

monitorTotalFailedProbes Total number of failed probes

monitorCurrentFailedProbes Total number of currently failed probes

stateflag stateflag

healthMonitor Monitor the health of this service. Available settings function as follows: YES - Send probes to check the health of the service. NO - Do not send probes to check the health of the service. With the NO option, the appliance shows the service as UP at all times.

appflowLog Enable logging of AppFlow information.

netProfile Network profile to use for the service.

svccfgFlags Contains the information about config info like internal/configured service

serviceIPstr This field has been intorduced to show the dbs services ip

state Initial state of the service.

weight The weight for the specified monitor.

svcMonFlags to store the flags of monitor bound to it

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

passive Indicates if load monitor is passive. A passive load monitor does not remove service from LB decision when threshold is breached.

oracleServerVersion Oracle server version

dnsProfileName Name of the DNS profile to be associated with the service. DNS profile properties will applied to the transactions processed by a service. This parameter is valid only for ADNS and ADNS-TCP services.

monConnectionClose Close monitoring connections by sending the service a connection termination message with the specified bit set.

noDefaultBindings to determine if the configuration will have default ssl CIPHER and ECC curve bindings

monUserStatusMesg This field has been introduced to show user monitor failure reasons

builtin feature The feature to be checked while applying this config

devno count

Example

The following is sample output of the show service -all command: 4 configured services: 1)

```
    svc1 (10.124.99.12:80) - HTTP        State: UP
```

Max Conn: 0 Max Req: 0 Use Source IP: NO Client Keepalive(CKA): NO TCP Buffering(TCPB): NO HTTP Compression(CMP): NO Idle timeout: Client: 180 sec Server: 360 sec Client IP: DISABLED 2) svc_3 (10.100.100.3:53) - DNS State: UP Max Conn: 0 Max Req: 0 Use Source IP: NO Client Keepalive(CKA): NO TCP Buffering(TCPB): NO HTTP Compression(CMP): NO Idle timeout: Client: 180 sec Server: 360 sec Client IP: DISABLED 3) tsvc1 (77.45.32.45:80) - HTTP State: UP Max Conn: 0 Max Req: 0 Use Source IP: NO Client Keepalive(CKA): NO TCP Buffering(TCPB): NO HTTP Compression(CMP): NO Idle timeout: Client: 180 sec Server: 360 sec Client IP: DISABLED 4) foosvc (10.124.99.13:7979) - HTTP State: UP Max Conn: 0 Max Req: 0 Use Source IP: NO Client Keepalive(CKA): NO TCP Buffering(TCPB): NO HTTP Compression(CMP): NO Idle timeout: Client: 180 sec Server: 360 sec Client IP: DISABLED

bind service

Binds a monitor to a service.

Synopsis

bind service <name>@ [-monitorName <string>@]

Arguments

name Name of the service to which to bind a monitor.

monitorName Name of the monitor to bind to the service.

monState Initial state of the service.

Possible values: ENABLED, DISABLED Default value: ENABLED

weight Weight to assign to the monitor-service binding. When a monitor is UP, the weight assigned to its binding with the service determines how much the monitor contributes toward keeping the health of the service above the value configured for the Monitor Threshold parameter. Default value: 1 Minimum value: 1 Maximum value: 100

passive Indicates if load monitor is passive. A passive load monitor does not remove service from LB decision when threshold is breached.

Example

bind service svc1 -monitorName mon1 To bind svc1, svc2 and svc3 to the monitor mon1 you can use the following command: bind service svc -monitorName mon1

serviceGroup

The following operations can be performed on "serviceGroup":

unset| enable| rename| bind| add| stat| unbind| show| disable| rm| set|

unset serviceGroup

Removes the attributes of the specified service group. Attributes for which a default value is available revert to their default values..Refer to the set serviceGroup command for meanings of the arguments.

Synopsis

unset serviceGroup <serviceGroupName>@ [<serverName>@]

Example

unset servicegroup http_svc_group -maxClient

enable serviceGroup

Enables a service group or a member of the service group.

Synopsis

enable serviceGroup <serviceGroupName>@

Arguments

serviceGroupName Name of the service group.

serverName Name of the server that hosts the service.

port Port number of the service to be enabled.

Example

enable servicegroup http_svc_group To enable multiple service groups at one go use the following command: enable servicegroup http_svc_group

rename serviceGroup

Renames a service group.

Synopsis

rename serviceGroup <serviceGroupName>@ <newName>@

Arguments

serviceGroupName Existing name of the service group.

newName New name for the service group.

Example

rename service svcgrp1 svcgrp-new1

bind serviceGroup

Binds a service to a service group.

Synopsis

bind serviceGroup <serviceGroupName> (<IP>@ | (<serverName>@) | ((-monitorName <string>@) | -CustomServerID <string> | -state (ENABLED | DISABLED) | -hashId <positive_integer> | | | -order <positive_integer>))

Arguments

serviceGroupName Name of the service group.

IP IP address of the server that hosts the service. Mutually exclusive with the Server Name parameter.

serverName Name of the server that hosts the service. Mutually exclusive with the IP address parameter.

port Port number of the service. Each service must have a unique port number.

monitorName The name of the service or a service group to which the monitor is to be bound.

monState Administrative state assigned to the monitor and service group binding. If set to disabled, the service group is not monitored.

Possible values: ENABLED, DISABLED Default value: ENABLED

passive Indicates if load monitor is passive. A passive load monitor does not remove service from LB decision when threshold is breached.

weight CustomServerID Unique service identifier. Used when the persistency type for the virtual server is set to Custom Server ID. Default value: "None"

state Initial state of the service after binding.

Possible values: ENABLED, DISABLED Default value: ENABLED

hashId Unique numerical identifier used by hash based load balancing methods to identify a service. Minimum value: 1

nameServer Specify the nameserver to which the query for bound domain needs to be sent. If not specified, use the global nameserver

dbsTTL Specify the TTL for DNS record for domain based service.The default value of ttl is 0 which indicates to use the TTL received in DNS response for monitors Default value: 0

order Order number to be assigned to the servicegroup member Minimum value: 1 Maximum value: 8192

Example

bind servicegroup http_svc_group 10.102.27.153 80 To bind multiple servers to a servicegroup, following command can be used: bind servicegroup http_svc_group 10.102.27. 80

add serviceGroup

Creates a service group. You can group similar services into a service group and use them as a single entity.

Synopsis

add serviceGroup <serviceGroupName>@ <serviceType> [-cip (ENABLED | DISABLED)] [-autoScale <autoScale> -memberPort <port>]

Arguments

serviceGroupName Name of the service group. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the name is created.

serviceType Protocol used to exchange data with the service.

Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, ADNS_TCP, MYSQL, MSSQL, ORACLE, MONGO, MONGO_TLS, RADIUS, RADIUSListener, RDP, DIAMETER, SSL_DIAMETER, TFTP, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, LOGSTREAM_SSL, MQTT, MQTT_TLS, QUIC_BRIDGE

cacheType Cache type supported by the cache server.

Possible values: TRANSPARENT, REVERSE, FORWARD

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

maxClient Maximum number of simultaneous open connections for the service group. Minimum value: 0 Maximum value: 4294967294

maxReq Maximum number of requests that can be sent on a persistent connection to the service group. Note: Connection requests beyond this value are rejected. Minimum value: 0 Maximum value: 65535

cacheable Use the transparent cache redirection virtual server to forward the request to the cache server. Note: Do not set this parameter if you set the Cache Type.

Possible values: YES, NO Default value: NO

cip Insert the Client IP header in requests forwarded to the service.

Possible values: ENABLED, DISABLED

cipHeader Name of the HTTP header whose value must be set to the IP address of the client. Used with the Client IP parameter. If client IP insertion is enabled, and the client IP header is not

specified, the value of Client IP Header parameter or the value set by the set ns config command is used as client's IP header name.

usip Use client's IP address as the source IP address when initiating connection to the server. With the NO setting, which is the default, a mapped IP (MIP) address or subnet IP (SNIP) address is used as the source IP address to initiate server side connections.

Possible values: YES, NO

pathMonitor Path monitoring for clustering

Possible values: YES, NO

pathMonitorIndv Individual Path monitoring decisions.

Possible values: YES, NO

useproxyport Use the proxy port as the source port when initiating connections with the server. With the NO setting, the client-side connection port is used as the source port for the server-side connection. Note: This parameter is available only when the Use Source IP (USIP) parameter is set to YES.

Possible values: YES, NO

healthMonitor Monitor the health of this service. Available settings function as follows: YES - Send probes to check the health of the service. NO - Do not send probes to check the health of the service. With the NO option, the appliance shows the service as UP at all times.

Possible values: YES, NO Default value: YES

sp Enable surge protection for the service group.

Possible values: ON, OFF Default value: OFF

rtspSessionidRemap Enable RTSP session ID mapping for the service group.

Possible values: ON, OFF Default value: OFF

cltTimeout Time, in seconds, after which to terminate an idle client connection. Maximum value: 31536000

svrTimeout Time, in seconds, after which to terminate an idle server connection. Maximum value: 31536000

CKA Enable client keep-alive for the service group.

Possible values: YES, NO

TCPB Enable TCP buffering for the service group.

Possible values: YES, NO

CMP Enable compression for the specified service.

Possible values: YES, NO

maxBandwidth Maximum bandwidth, in Kbps, allocated for all the services in the service group. Minimum value: 0 Maximum value: 4294967287

monThreshold Minimum sum of weights of the monitors that are bound to this service. Used to determine whether to mark a service as UP or DOWN. Minimum value: 0 Maximum value: 65535

state Initial state of the service group.

Possible values: ENABLED, DISABLED Default value: ENABLED

downStateFlush Flush all active transactions associated with all the services in the service group whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions.

Possible values: ENABLED, DISABLED Default value: ENABLED

tcpProfileName Name of the TCP profile that contains TCP configuration settings for the service group.

httpProfileName Name of the HTTP profile that contains HTTP configuration settings for the service group.

comment Any information about the service group.

appflowLog Enable logging of AppFlow information for the specified service group.

Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile Network profile for the service group.

autoScale Auto scale option for a servicegroup

Possible values: DISABLED, DNS, POLICY, CLOUD, API Default value: DISABLED

memberPort member port

autoDisablegraceful Indicates graceful shutdown of the service. System will wait for all outstanding connections to this service to be closed before disabling the service.

Possible values: YES, NO Default value: NO

autoDisabledelay The time allowed (in seconds) for a graceful shutdown. During this period, new connections or requests will continue to be sent to this service for clients who already have a persistent session on the system. Connections or requests from fresh or new clients who do not yet have a persistence sessions on the system will not be sent to the service. Instead, they will be load balanced among other available services. After the delay time expires, no new requests or connections will be sent to the service.

autoDelayedTrofs Indicates graceful movement of IP-Port binding/s to TROFS when IP addresses are removed from DNS response. System will wait for monitor response timeout period before moving to TROFS .

Possible values: YES, NO Default value: NO

monConnectionClose Close monitoring connections by sending the service a connection termination message with the specified bit set.

Possible values: RESET, FIN Default value: NONE

Example

add servicegroup http_svc_group http To add service groups sgrp1, sgrp2 and sgrp3 at one go use the following command: add servicegroup sgrp http

stat serviceGroup

Displays configuration statistics of the specified service group or all the service groups configured on the appliance.

Synopsis

stat serviceGroup

Arguments

serviceGroupName Name of the service group for which to display settings.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

State Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)

Service type (Type) The service type of this service.Possible values are ADNS, DNS, MYSQL, RTSP, SSL_DIAMETER, ADNS_TCP, DNS_TCP, NNTP, SIP_UDP, SSL_TCP, ANY, FTP, RADIUS, SNMP, TCP, DHCPRA, HTTP, RDP, SSL, TFTP, DIAMETER, MSSQL, RPCSVR, SSL_BRIDGE, UDP

Related Commands

- stat serviceGroupMember

unbind serviceGroup

Unbinds a service or a monitor from a service group.

Synopsis

unbind serviceGroup <serviceGroupName> (<IP>@ | <serverName>@ | -monitorName <string>@)

Arguments

serviceGroupName Name of the service group.

IP IP address of the server that hosts the service. Mutually exclusive with the Server Name parameter.

serverName Name of the server that hosts the service. Mutually exclusive with the IP Address parameter.

port Port number of the service.

monitorName Name of the monitor to bind to the service group.

Example

unbind servicegroup http_svc_group 10.102.27.153 80 To unbind multiple servers following command can be used: unbind servicegroup http_svc_group 10.102.27. 80

show serviceGroup

Displays the specified service group's binding information.

Synopsis

show serviceGroup

Arguments

serviceGroupName Name of the service group.

includeMembers Display the members of the listed service groups in addition to their settings. Can be specified when no service group name is provided in the command. In that case, the details displayed for each service group are identical to the details displayed when a service group name is provided, except that bound monitors are not displayed.

Output

numOfconnections This will tell the number of client side connections are still open.

numOfCurConnections This will tell number of current client connections

numOfLastConnections This will tell number of connections that are linked by last connection

serviceType Protocol used to exchange data with the service.

port The port number of the service to be enabled.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

serviceConfTpye serviceConfType The configuration type of the service group.

value SSL Status.

cacheType Cache type supported by the cache server.

maxClient Maximum number of simultaneous open connections for the service group.

maxReq Maximum number of requests that can be sent on a persistent connection to the service group. Note: Connection requests beyond this value are rejected.

cacheable The state of cache on the service.

cip Insert the Client IP header in requests forwarded to the service.

cipHeader CIP Header.

usip Use client's IP address as the source IP address when initiating connection to the server. With the NO setting, which is the default, a mapped IP (MIP) address or subnet IP (SNIP) address is used as the source IP address to initiate server side connections.

pathMonitor Path monitoring for clustering

pathMonitorIndv Individual Path monitoring decisions.

useproxyport The use of client's Port.

monweight weight of the monitor that is bound to servicegroup.

sp Enable surge protection for the service group.

rtspSessionidRemap Enable RTSP session ID mapping for the service group.

cltTimeout Time, in seconds, after which to terminate an idle client connection.

svrTimeout Time, in seconds, after which to terminate an idle server connection.

CKA Enable client keep-alive for the service group.

TCPB Enable TCP buffering for the service group.

CMP Enable compression for the specified service.

maxBandwidth Maximum bandwidth, in Kbps, allocated for all the services in the service group.

state The state of the service group

svrState The state of the service

delay The remaining time in seconds for the service to be disabled

delay The remaning time in seconds for the service to be disabled

IP IP Address.

serverName The name of the server to be changed.

monitorName Monitor name.

monThreshold Minimum sum of weights of the monitors that are bound to this service. Used to determine whether to mark a service as UP or DOWN.

monState Monitor state.

weight CustomServerID The identifier for this IP:Port pair. Used when the persistency type is set to Custom Server ID.

serverID The identifier for the service. This is used when the persistency type is set to Custom Server ID.

monState The running state of the monitor on this service.

monStatCode The code indicating the monitor response.

monStatParam1 First parameter for use with message code.

monStatParam2 Second parameter for use with message code.

monStatParam3 Third parameter for use with message code.

monitorTotalProbes Total number of probes sent to monitor this service.

monitorTotalFailedProbes Total number of failed probes

monitorCurrentFailedProbes Total number of currently failed probes

downStateFlush Flush all active transactions associated with all services in the service group whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions.

lastresponse The string form of monstatcode.

stateChangeTimeSec Time when last state change occurred. Seconds part.

stateChangeTimemSec Time when last state change occurred. Milliseconds part.

timeSinceLastStateChange Time in milliseconds since the last state change.

ticksSinceLastStateChange Time in 10 millisecond ticks since the last state change.

StateUpdateReason Checks state update reason on the secondary node.

ClMonOwner Tells the mon owner of the service.

ClMonView Tells the view id of the monitoring owner.

groupCount Servicegroup Count

comment Any information about the service group.

tcpProfileName Name of the TCP profile that contains TCP configuration settings for the service group.

httpProfileName Name of the HTTP profile that contains HTTP configuration settings for the service group.

hashId The hash identifier for the service. This must be unique for each service. This parameter is used by hash based load balancing methods.

graceFul Indicates graceful shutdown of the service. System will wait for all outstanding connections to this service to be closed before disabling the service.

healthMonitor Monitor the health of this service. Available settings function as follows: YES - Send probes to check the health of the service. NO - Do not send probes to check the health of the service. With the NO option, the appliance shows the service as UP at all times.

appflowLog Enable logging of AppFlow information for the specified service group.

netProfile Network profile for the service group.

autoScale Auto scale option for a servicegroup

memberPort member port

autoDisablegraceful Indicates graceful shutdown of the service. System will wait for all outstanding connections to this service to be closed before disabling the service.

autoDisabledelay The time allowed (in seconds) for a graceful shutdown. During this period, new connections or requests will continue to be sent to this service for clients who already have a persistent session on the system. Connections or requests from fresh or new clients who do not yet have a persistence sessions on the system will not be sent to the service. Instead, they will be load balanced among other available services. After the delay time expires, no new requests or connections will be sent to the service.

autoDelayedTrofs Indicates graceful movement of IP-Port binding/s to TROFS when IP addresses are removed from DNS response. System will wait for monitor response timeout period before moving to TROFS .

state Monitor state.

weight weight of the monitor that is bound to servicegroup.

serviceIPstr This field has been intorduced to show the dbs services ip

serviceGroupEntName2 passive Indicates if load monitor is passive. A passive load monitor does not remove service from LB decision when threshold is breached.

serviceGroupeffectivestate Indicates the effective servicegroup state based on the state of the bound service items.If all services are UP the effective state is UP, if all are DOWN its DOWN,if all are OFS its OFS.If atleast one serviceis UP and rest are either DOWN or OFS, the effective state is PARTIAL-UP.If atleast one bound service is DOWN and rest are OFS the effective state is PARTIAL DOWN.

monConnectionClose Close monitoring connections by sending the service a connection termination message with the specified bit set.

noDefaultBindings to determine if the configuration is from stylebooks

nameServer Specify the nameserver to which the query for bound domain needs to be sent. If not specified, use the global nameserver

dbsTTL Specify the TTL for DNS record for domain based service.The default value of ttl is 0 which indicates to use the TTL received in DNS response for monitors

svcitmActSvcs This gives the total active service items for an FQDN for SRV type server binding

svcitmPriority This gives the priority of the FQDN service items for SRV server binding

svcitmBoundSvcs This gives the total bound items for an FQDN for SRV type server binding

responseTime Response time of this monitor in milli sec.

members Desired servicegroupmember binding set. Any existing servicegroupmember which is not part of the input will be deleted or disabled based on graceful setting on servicegroup.

failedmembers List of servicegroupmembers which couldn't be bound.

trofsReason Specify reason if service group member in TROFS

monUserStatusMesg This field has been introduced to show user monitor failure reasons

order Order number to be assigned to the servicegroup member

order Order number in string form to be assigned to the servicegroup member

trofsDelay Delay before moving to TROFS

devno count stateflag

disable serviceGroup

Disables a service group or a member of a service group. To disable a service group, provide only the service group name. To disable only a member of a service group, in addition to the service group name, provide the name of the server that hosts the service, and the port number of the service.

Synopsis

disable serviceGroup <serviceGroupName>@

Arguments

serviceGroupName Name of the service group.

serverName Name of the server that hosts the service.

port Port number of the service.

delay Time, in seconds, allocated for a shutdown of the services in the service group. During this period, new requests are sent to the service only for clients who already have persistent sessions on the appliance. Requests from new clients are load balanced among other available services. After the delay time expires, no requests are sent to the service, and the service is marked as unavailable (OUT OF SERVICE).

graceFul Wait for all existing connections to the service to terminate before shutting down the service.

Possible values: YES, NO Default value: NO

Example

disable servicegroup http_svc_group 10.102.27.153 80 -delay 10 To disable multiple servicegroups use the following command: disable servicegroup http_svc_group 10.102.27. 80 -delay 30

rm serviceGroup

Removes a service group.

Synopsis

rm serviceGroup <serviceGroupName>@

Arguments

serviceGroupName Name of the service group.

Example

rm servicegroup http_svc_group To remove multiple servicegroups at once, the following command can be used: rm servicegroup http_svc_group

set serviceGroup

Modifies the specified parameters of a service group.

Synopsis

set serviceGroup <serviceGroupName>@ [(<serverName>@) | -maxClient <positive_integer> | -maxReq <positive_integer> | -cacheable (YES | NO) | -cip (ENABLED | DISABLED) | <cipHeader> | -usip (YES | NO) | -useproxyport (YES | NO) | -sp (ON | OFF) | -rtspSessionidRemap (ON | OFF) | -cltTimeout <secs> | -svrTimeout <secs> | -CKA (YES | NO) | -TCPB (YES | NO) | -CMP (YES | NO) | -maxBandwidth <positive_integer> | -monThreshold <positive_integer> | -downStateFlush (ENABLED | DISABLED)]

Arguments

serviceGroupName Name of the service group.

serverName Name of the server to which to bind the service group.

port Server port number.

weight Weight to assign to the servers in the service group. Specifies the capacity of the servers relative to the other servers in the load balancing configuration. The higher the weight, the higher the percentage of requests sent to the service. Minimum value: 1 Maximum value: 100

CustomServerID The identifier for this IP:Port pair. Used when the persistency type is set to Custom Server ID. Default value: "None"

hashId The hash identifier for the service. This must be unique for each service. This parameter is used by hash based load balancing methods. Minimum value: 1

nameServer Specify the nameserver to which the query for bound domain needs to be sent. If not specified, use the global nameserver

dbsTTL Specify the TTL for DNS record for domain based service.The default value of ttl is 0 which indicates to use the TTL received in DNS response for monitors Default value: 0

order Order number to be assigned to the servicegroup member Minimum value: 1 Maximum value: 8192

monitorName Name of the monitor bound to the service group. Used to assign a weight to the monitor.

weight weight of the monitor that is bound to servicegroup. Minimum value: 1

maxClient Maximum number of simultaneous open connections for the service group. Minimum value: 0 Maximum value: 4294967294

maxReq Maximum number of requests that can be sent on a persistent connection to the service group. Note: Connection requests beyond this value are rejected. Minimum value: 0 Maximum value: 65535

healthMonitor Monitor the health of this service. Available settings function as follows: YES - Send probes to check the health of the service. NO - Do not send probes to check the health of the service. With the NO option, the appliance shows the service as UP at all times.

Possible values: YES, NO Default value: YES

cacheable Use the transparent cache redirection virtual server to forward the request to the cache server. Note: Do not set this parameter if you set the Cache Type.

Possible values: YES, NO Default value: NO

cip Insert the Client IP header in requests forwarded to the service.

Possible values: ENABLED, DISABLED

cipHeader CIP Header.

usip Use client's IP address as the source IP address when initiating connection to the server. With the NO setting, which is the default, a mapped IP (MIP) address or subnet IP (SNIP) address is used as the source IP address to initiate server side connections.

Possible values: YES, NO

pathMonitor Path monitoring for clustering

Possible values: YES, NO

pathMonitorIndv Individual Path monitoring decisions.

Possible values: YES, NO

useproxyport Use the proxy port as the source port when initiating connections with the server. With the NO setting, the client-side connection port is used as the source port for the server-side connection. Note: This parameter is available only when the Use Source IP (USIP) parameter is set to YES.

Possible values: YES, NO

sp Enable surge protection for the service group.

Possible values: ON, OFF Default value: OFF

rtspSessionidRemap Enable RTSP session ID mapping for the service group.

Possible values: ON, OFF Default value: OFF

cltTimeout Time, in seconds, after which to terminate an idle client connection. Maximum value: 31536000

svrTimeout Time, in seconds, after which to terminate an idle server connection. Maximum value: 31536000

CKA Enable client keep-alive for the service group.

Possible values: YES, NO

TCPB Enable TCP buffering for the service group.

Possible values: YES, NO

CMP Enable compression for the specified service.

Possible values: YES, NO

maxBandwidth Maximum bandwidth, in Kbps, allocated for all the services in the service group. Minimum value: 0 Maximum value: 4294967287

monThreshold Minimum sum of weights of the monitors that are bound to this service. Used to determine whether to mark a service as UP or DOWN. Minimum value: 0 Maximum value: 65535

downStateFlush Flush all active transactions associated with all the services in the service group whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions.

Possible values: ENABLED, DISABLED Default value: ENABLED

tcpProfileName Name of the TCP profile that contains TCP configuration settings for the service group.

httpProfileName Name of the HTTP profile that contains HTTP configuration settings for the service group.

comment Any information about the service group.

appflowLog Enable logging of AppFlow information for the specified service group.

Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile Network profile for the service group.

autoDisablegraceful Indicates graceful shutdown of the service. System will wait for all outstanding connections to this service to be closed before disabling the service.

Possible values: YES, NO Default value: NO

autoDisabledelay The time allowed (in seconds) for a graceful shutdown. During this period, new connections or requests will continue to be sent to this service for clients who already have a persistent session on the system. Connections or requests from fresh or new clients who do not yet have a persistence sessions on the system will not be sent to the service. Instead, they will be

load balanced among other available services. After the delay time expires, no new requests or connections will be sent to the service.

autoDelayedTrofs Indicates graceful movement of IP-Port binding/s to TROFS when IP addresses are removed from DNS response. System will wait for monitor response timeout period before moving to TROFS .

Possible values: YES, NO Default value: NO

monConnectionClose Close monitoring connections by sending the service a connection termination message with the specified bit set.

Possible values: RESET, FIN Default value: NONE

autoScale Set this parameter to API to enable using Desired State API for binding intended servicegroup member set. Setting this parameter to API may result in error if the already existing member bindings fall under below category -

1. Domain based server
2. Named servers
3. servers whose name and IP do not match. example: add server 1.2.3.4 4.3.2.1
4. Loopback servers should be named only 127.0.0.1 or 0000:0000:0000:0000:0000:0000:0000:0001.

Possible values: DISABLED, DNS, POLICY, CLOUD, API Default value: DISABLED

Example

set servicegroup http_svc_group -maxClient 100 To set the attribute maxclient for multiple servicegroups at once, use the following command: set servicegroup http_svc_group -maxClient 100

serviceGroupMember

The following operations can be performed on "serviceGroupMember":

stat serviceGroupMember

Display statistics of a service group member.

Synopsis

stat serviceGroupMember <serviceGroupName> (<IP> | <serverName>)

Arguments

serviceGroupName Displays statistics for the specified service group.Name of the service group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my servicegroup" or 'my servicegroup').

IP IP address of the service group. Mutually exclusive with the server name parameter.

serverName Name of the server. Mutually exclusive with the IP address parameter.

port Port number of the service group member.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Average server TTFB (SvrTTFB) Average TTFB between the Citrix ADC and the server. TTFB is the time interval between sending the request packet to a service and receiving the first response from the service

IP address (IP) The IP address on which the service is running.

Port (port) The port on which the service is running.

Service type (Type) The service type of this service.Possible values are ADNS, DNS, MYSQL, RTSP, SSL_DIAMETER, ADNS_TCP, DNS_TCP, NNTP, SIP_UDP, SSL_TCP, ANY, FTP, RADIUS, SNMP, TCP, DHCPRA, HTTP, RDP, SSL, TFTP, DIAMETER, MSSQL, RPCSVR, SSL_BRIDGE, UDP

State Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)

Service Group Member Binding Order (Order) Order with which service group member is bound to service group

Requests (Req) Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Responses (Rsp) Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Request bytes (Reqb) Total number of request bytes received on this service or virtual server.

Response bytes (Rspb) Number of response bytes received by this service or virtual server.

Current client connections (ClntConn) Number of current client connections.

Requests in surge queue (SurgeQ) Number of requests in the surge queue.

Current server connections (SvrConn) Number of current connections to the actual servers behind the virtual server.

Current Server Est connections (SvrEstConn) Number of server connections in ESTABLISHED state.

Connections in reuse pool (ReuseP) Number of requests in the idle queue/reuse pool.

Maximum server connections (MaxConn) Maximum open connections allowed on this service.

No of TCPConn ReasmQ 75% reached (ReassQ75) Total no of connections with 75% TCP reassembly queue

No of TCPConn ReasmQ Flushed (ReassQFlush) Total no of connections incurred TCP reassembly queue flush

Total transactions for server TTLB (totSvrTTLBTransactions) Total transactions where server TTLB is calculated.

Tolerating TTLB Transactions (toleratingTTLBTransactions) Tolerable transactions based on APDEX threshold (>T && <4T).

Frustrating TTLB Transactions (frustratingTTLBTransactions) Frustrating transactions based on APDEX threshold (>4T).

Current load on the service (Load) Load on the service that is calculated from the bound load based monitor.

No of http max header size packet parsing failures (httpMaxHdrSzPkts) Number of http max header size packet parsing failures

Number of HTTP requests exceeding max header field length (httpMaxHdrFldLenPkts) Number of HTTP requests exceeding max header field length

max ooo packets threshold hits (tcpMaxoooPkts) No of times max out of order packets reached

Binding Order (Order) Order with which service is bound to vserver

servicegroupbindings

The following operations can be performed on "servicegroupbindings":

show servicegroupbindings

Displays servicegroup information followed by vservers bound to it.

Synopsis

show servicegroupbindings <serviceGroupName>

Arguments

serviceGroupName The name of the service.

Output

IPAddress The IP address of the vserver.

port The port of the vserver.

state The state of the service group

svrState The state of the vserver

vServerName The name of the vserver.

stateflag devno count

svcbindings

The following operations can be performed on "svcbindings":

show svcbindings

Displays a list of all virtual servers to which the service is bound.

Synopsis

show svcbindings <serviceName>

Arguments

serviceName The name of the service.

Output

IPAddress The IP address of the vserver.

port The port of the vserver.

svrState The state of the vserver

vServerName The name of the vserver.

stateflag devno count

systemLevelReporting

The following operations can be performed on "systemLevelReporting":

enable| disable| show|

enable systemLevelReporting

This operation will enable system level reporting

Synopsis

enable systemLevelReporting

disable systemLevelReporting

This operation would disable system level reporting

Synopsis

disable systemLevelReporting

show systemLevelReporting

This operation gets the system level reporting state

Synopsis

show systemLevelReporting

Arguments

Output

reportingMode Shows whether system level reporting is enabled/disabled

uiinternal

The following operations can be performed on "uiinternal":

unset| show| set|

unset uiinternal

unset uiinternal for the entities.Refer to the set uiinternal command for meanings of the arguments.

Synopsis

unset uiinternal <entityType> <name>

Example

unset uiinternal lbvserver v1 -template app1

show uiinternal

display all UI internal data information for the entities

Synopsis

show uiinternal

Arguments

entityType The entitiy type of UI internal data

Possible values: LBVSERVER, GSLBVSERVER, CRVSERVER, VPNVSERVER, CSVSERVER, AUTHENTICATIONVSERVER, SERVER, SERVICE, SERVICEGROUP, GSLBSERVICE, EXPRESSION, VPNURL

name The entity name

Output

template The template associated with the entity

comment The comment associated with the entity

uiinfo The uiinfo associated with the entity

rule The rule associated with the entity

dnsSecurityTag DNS Security tag asscociated with the entity

devno count stateflag

Example

show uiinternal LBVSERVER v1

set uiinternal

set uiinternal data for the entities

Synopsis

set uiinternal <entityType> <name>

Arguments

entityType The entitiy type of UI internal data

Possible values: LBVSERVER, GSLBVSERVER, CRVSERVER, VPNVSERVER, CSVSERVER, AUTHENTICATIONVSERVER, SERVER, SERVICE, SERVICEGROUP, GSLBSERVICE, EXPRESSION, VPNURL

name The entity name

template The application template associated with entity

comment The application template associated with entity

rule rules associated with entity

dnsSecurityTag DNS Security tag asscociated with the entity Minimum value: 0

Example

set uiinternal lbvserver v1 -template app1

vserver

The following operations can be performed on "vserver":

set| show| unset| rm| disable| enable|

set vserver

Use this command to modify the parameters for an existing virtual server. NOTE: This command is deprecated.This command is deprecated in 10.0, instead you can use commands such as set lb vserver

Synopsis

Arguments

name The name of the virtual server for which the parameters are to be set.

pushVserver The lb vserver of type PUSH/SSL_PUSH to which server pushes the updates received on the client facing non-push lb vserver.

Example

set vserver lb_vip -backupVServerName bkvip_lbvip To set backup vserver for multiple vservers at once, use the following command: set vserver lb_vip -backupVServerName bkvip_lbvip

show vserver

Displays information about all virtual servers configured on the appliance.

Synopsis

show vserver

Example

show vserver lb_vip

unset vserver

Use this command to unset the backup virtual server or the redirectURL that has been set on the virtual server..Refer to the set vserver command for meanings of the arguments.NOTE: This command is deprecated.

Synopsis

Example

unset vserver lb_vip -backupVServer To unset the backup vserver for multiple vservers use the following command: unset vserver lb_vip -backupVServer

rm vserver

Use this command to remove a virtual server. NOTE: This command is deprecated.This command is deprecated in 10.0, instead you can use commands such as rm lb vserver

Synopsis

Arguments

name The name of the virtual server to be removed.

Example

rm vserver lb_vip To remove multiple vservers, use the following command: rm vserver lb_vip

disable vserver

Use this command to disable (take out of service) a virtual server. NOTE: This command is deprecated.This command is deprecated in 10.0, instead you can use commands such as disable lb vserver

Synopsis

Arguments

name The name of the virtual server to be disabled. Notes: 1.The system will continue to respond to ARP and/or ping requests for the IP address of this virtual server. 2.As the virtual server is still

configured in the system, you can enable the virtual server using the ###enable vserver### command.

Example

disable vserver lb_vip To disable multiple vservers, use the following command: disable vserver lb_vip

enable vserver

Use this command to enable a virtual server. Note: Virtual servers, when added, are enabled by default. NOTE: This command is deprecated.This command is deprecated in 10.0, instead you can use commands such as enable lb vserver

Synopsis

Arguments

name The name of the virtual server to be enabled.

Example

enable vserver lb_vip To enable multiple vservers, use the following command: enable vserver lb_vip

botmgmt

bot-global

The following operations can be performed on "bot-global":

bind| show| unbind|

bind bot global

Activates the specified bot policy for all requests sent to the Citrix ADC.

Synopsis

bind bot global -policyName <string> -priority <positive_integer>

Arguments

policyName Name of the bot policy to activate. If you want to create the policy as well as activate it, specify a name for the bot policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my bot policy" or 'my bot policy').

priority Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Must be unique within the label. Policies are evaluated in the order of their priority numbers, and the first policy that matches the request is applied. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.

- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.
- The expression evaluates to a priority number that is smaller than the current policy's priority number.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

type Bind point to which to bind the policy. Available settings function as follows:

- REQ_OVERRIDE - Request override. Binds the policy to the priority request queue.
- REQ_DEFAULT - Binds the policy to the default request queue.

Possible values: REQ_OVERRIDE, REQ_DEFAULT

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server.

labelType Type of invocation, Available settings function as follows:

- vserver - Forward the request to the specified virtual server.
- policylabel - Invoke the specified policy label.

Possible values: vserver, policylabel

labelName Name of the policy label to invoke. If the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is policylabel.

Example

i)bind bot global -policyName pol9 -priority 9

show bot global

Displays the list of policies bound to the specified bot global bind point. If no bind point is specified, displays a list of all policies bound to bot global.

Synopsis

show bot global

Arguments

type Specifies the bind point whose policies you want to display. Available settings function as follows:

- REQ_OVERRIDE - Request override. Binds the policy to the priority request queue.
- REQ_DEFAULT - Binds the policy to the default request queue.

Possible values: REQ_OVERRIDE, REQ_DEFAULT

Output

stateflag policyName Name of the bot policy.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server.

labelType Type of invocation, Available settings function as follows:

- vserver - Forward the request to the specified virtual server.
- policylabel - Invoke the specified policy label.

labelName Name of the policy label to invoke. If the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is policylabel.

flowType flowtype of the bound bot policy.

numpol number of polices bound to label.

flags globalBindType devno count

Example

show bot global

unbind bot global

Unbind the specified bot policy from bot global.

Synopsis

unbind bot global -policyName <string>

Arguments

policyName Name of the policy to unbind.

type The bindpoint from which the policy is to be unbound.

Possible values: REQ_OVERRIDE, REQ_DEFAULT

priority Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind bot global -policyName pol9

bot-policy

The following operations can be performed on "bot-policy":

set| show| unset| stat| rename| add| rm|

set bot policy

Modifies the rule or action portion of the specified bot policy.

Synopsis

set bot policy <name>

Arguments

name Name of the bot policy.

rule Expression that the policy uses to determine whether to apply bot profile on the specified request.

profileName Name of the bot profile to apply if the request matches this bot policy.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition.

comment Any type of information about this bot policy.

logAction Name of the messagelog action to use for requests that match this policy.

Example

set bot policy pol9 -rule "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh2\\")"

show bot policy

Displays the current settings for the specified bot policy. If no policy name is specified, displays a list of all bot policies currently configured on the Citrix ADC, with abbreviated settings.

Synopsis

show bot policy show bot policy stats - alias for 'stat bot policy'

Arguments

name Name of the bot policy for which to display settings.

Output

stateflag rule Expression that the policy uses to determine whether to apply bot profile on the specified request.

profileName Name of the bot profile to apply if the request matches this bot policy.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition.

hits Number of hits.

undefHits Number of policy UNDEF hits.

activePolicy Indicates whether policy is bound or not.

boundTo Location where policy is bound

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

comment Any type of information about this bot policy.

logAction Name of the messagelog action to use for requests that match this policy.

bindPolicyType vserverType builtin Flag to determine if bot policy is built-in or not

feature The feature to be checked while applying this config

type devno count

Example

show bot policy

unset bot policy

Removes the settings of an existing bot policy. Attributes for which a default value is available revert to their default values..Refer to the set bot policy command for meanings of the arguments.

Synopsis

unset bot policy <name>

Example

unset bot policy botpol9 -undefAction

stat bot policy

Displays statistics for all bot policies currently configured on the Citrix ADC, or detailed statistics for the specified policy.

Synopsis

stat bot policy

Arguments

name Name of the bot policy for which to show detailed statistics.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Policy undef hits (Undefhits) Number of undef hits on the policy

Related Commands

- stat bot policylabel

rename bot policy

Renames the specified bot policy.

Synopsis

rename bot policy <name>@ <newName>@

Arguments

name Existing name of the bot policy.

newName New name for the bot policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my bot policy" or 'my bot policy').

Example

rename bot policy oldname newname

add bot policy

Creates a bot policy.

Synopsis

add bot policy <name> -rule <expression> -profileName <string>

Arguments

name Name for the bot policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the bot policy is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my bot policy" or 'my bot policy').

rule Expression that the policy uses to determine whether to apply bot profile on the specified request.

profileName Name of the bot profile to apply if the request matches this bot policy.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition.

comment Any type of information about this bot policy.

logAction Name of the messagelog action to use for requests that match this policy.

Example

i) add bot policy pol9 -rule "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh3\\")" -profileName bot_prof

rm bot policy

Removes the specified bot policy.

Synopsis

rm bot policy <name>

Arguments

name Name of the bot policy to remove.

Example

rm bot policy pol9

bot-policylabel

The following operations can be performed on "bot-policylabel":

bind| unbind| stat| rename| show| rm| add|

bind bot policylabel

Binds the specified bot policy to the specified policy label.

Synopsis

bind bot policylabel <labelName> -policyName <string> -priority <positive_integer>

Arguments

labelName Name of the bot policy label to which to bind the policy.

policyName Name of the policy to bind to the bot policy label.

priority Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Must be unique within the label. Policies are evaluated in the order of their priority numbers, and the first policy that matches the request is applied. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.
- The expression evaluates to a priority number that is smaller than the current policys priority number.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label and evaluate the specified policy label.

labelType Type of policy label to invoke. Available settings function as follows:

- vserver - Invoke an unnamed policy label associated with a virtual server.
- policylabel - Invoke a user-defined policy label.

Possible values: vserver, policylabel

labelName

- If labelType is policylabel, name of the policy label to invoke.
- If labelType is vserver, name of the virtual server.

Example

i)bind bot policylabel resp_lab pol_resp 1 2 ii)bind bot policylabel resp_lab pol_resp 1 2 -invoke vserver CURRENT

unbind bot policylabel

Unbinds the specified bot policy from the specified policy label.

Synopsis

unbind bot policylabel <labelName> -policyName <string>

Arguments

labelName Name for the bot policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the responder policy label is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder policy label" or my responder policy label').

policyName The name of the policy to be unbound.

priority Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind bot policylabel bot_lab pol_bot

stat bot policylabel

Displays statistics for the specified bot policy label. If no policy label name is provided, displays abbreviated statistics for all bot policy labels currently configured on the Citrix ADC.

Synopsis

stat bot policylabel

Arguments

labelName Name of the bot policy label.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy Label Hits (Hits) Number of times policy label was invoked.

Related Commands

- stat bot profile

rename bot policylabel

Renames the specified bot policy label.

Synopsis

rename bot policylabel <labelName>@ <newName>@

Arguments

labelName Current name of the bot policy label.

newName New name for the bot policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

Example

rename bot policylabel oldname newname

show bot policylabel

Displays the current settings for the specified bot policy label. If no policy label is specified, displays a list of all bot policy labels currently configured on the Citrix ADC, with abbreviated settings.

Synopsis

show bot policylabel

Arguments

labelName Name of the bot policy label.

Output

stateflag numpol number of polices bound to label.

hits Number of times policy label was invoked.

policyName Name of the bot policy.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label and evaluate the specified policy label.

labelType Type of policy label to invoke. Available settings function as follows:

- vserver - Invoke an unnamed policy label associated with a virtual server.
- policylabel - Invoke a user-defined policy label.

labelName

- If labelType is policylabel, name of the policy label to invoke.
- If labelType is vserver, name of the virtual server.

flags policylabeltype Type of transformations allowed by the policies bound to the label.

comment Any comments to preserve information about this bot policy label.

devno count

Example

i)show bot policylabel bot_lab ii)show bot policylabel

rm bot policylabel

Removes a bot policy label.

Synopsis

rm bot policylabel <labelName>

Arguments

labelName Name of the bot policy label to remove.

Example

rm bot policylabel bot_lab

add bot policylabel

Creates a user-defined bot policy label, to which you can bind policies. A policy label is a tool for evaluating a set of policies in a specified order. By using a policy label, you can configure the responder feature to choose the next policy, invoke a different policy label, or terminate policy evaluation completely by looking at whether the previous policy evaluated to TRUE or FALSE.

Synopsis

add bot policylabel <labelName>

Arguments

labelName Name for the bot policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the responder policy label is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder policy label" or my responder policy label').

comment Any comments to preserve information about this bot policy label.

Example

add bot policylabel bot_lab

bot-profile

The following operations can be performed on "bot-profile":

unset| stat| bind| set| show| add| unbind| rm|

unset bot profile

Use this command to remove bot profile settings.Refer to the set bot profile command for meanings of the arguments.

Synopsis

unset bot profile <name>

stat bot profile

Displays statistics for the specified bot profile. If no profile is specified, displays abbreviated statistics for all the profiles.

Synopsis

stat bot profile

Arguments

name Name of the bot profile.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

requests (reqs) HTTP/HTTPS requests sent to your protected web servers via the Bot profile.

Request Bytes (reqBytes) Number of bytes transfered for requests

responses (resps) HTTP/HTTPS responses sent by your protected web servers via the Bot profile.

Response Bytes (resBytes) Number of bytes transfered for responses

total logs profile (botLogProfile) Total number of logs by the Bot profile.

total drop profile (botDropProfile) Total number of drops by the Bot profile.

total redirect profile (botRedirectProfile) Total number of redirects by the Bot profile.

total reset profile (botResetProfile) Total number of resets by the Bot profile.

Device Fingerprint (deviceFingerPrintProfile) Number of device fingerprint violations seen by the Bot profile.

Device Fingerprint Logs (deviceFingerPrintLogProfile) Number of device fingerprint violations logged by the Bot profile.

Device Fingerprint Drop (deviceFingerPrintDropProfile) Number of device fingerprint violations dropped by the Bot profile.

Device Fingerprint Redirect (deviceFingerPrintRedirectProfile) Number of device fingerprint violations requests redirected by the Bot profile to a different Web page or web server.

Device Fingerprint Captcha (deviceFingerPrintCaptchaProfile) Number of device fingerprint violation requests for which CAPTCHA challenge was sent due to Bot profile.

Device Fingerprint Reset (deviceFingerPrintResetProfile) Number of device fingerprint violations reset by the Bot profile.

IP Reputation (ipRepProfile) Number of ip reputation violations seen by the Bot profile.

IP Reputation Logs (ipRepLogProfile) Number of ip reputation violations logged by the Bot Profile.

IP Reputation Drop (ipRepDropProfile) Number of ip reputation violations dropped by the Bot profile.

IP Reputation Redirect (ipRepRedirectProfile) Number of ip reputation violations requests redirected by the Bot profile to a different Web page or web server.

IP Reputation Captcha (ipRepCaptchaProfile) Number of ip reputation violation requests for which CAPTCHA challenge was sent due to Bot profile.

IP Reputation Reset (ipRepResetProfile) Number of ip reputation violations reset by the Bot profile.

White List (whiteListProfile) Number of white list violations seen by the Bot profile.

White List Logs (whiteListLogProfile) Number of white list violations logged by the Bot profile.

Black List (blackListProfile) Number of black list violations seen by the Bot profile.

Black List Logs (blackListLogProfile) Number of black list violations logged by the Bot profile.

Black List Drop (blackListDropProfile) Number of black list violations dropped by the Bot profile.

Black List Reset (blackListResetProfile) Number of black list violations reset by the Bot profile.

Black List Redirect (blackListRedirectProfile) Number of black list violations redirected by the Bot profile to a different Web page or web server.

Rate Limit (rateLimitProfile) Number of rate limiting violations seen by the Bot profile.

Rate Limit Logs (rateLimitLogProfile) Number of rate limiting violations logged by the Bot profile.

Rate Limit Drop (rateLimitDropProfile) Number of rate limiting violations dropped by the Bot profile.

Rate Limit Redirect (rateLimitRedirectProfile) Number of rate limiting violations requests redirected by the Bot profile to a different Web page or web server.

Rate Limit Reset (rateLimitResetProfile) Number of rate limiting violations reset by the Bot profile.

Static Signature (staticSignnatureProfile) Number of static signatutre violations seen by the Bot profile.

Static Signature Logs (staticSignnatureLogProfile) Number of static signatutre violations logged by the Bot profile.

Static Signature Drop (staticSignnatureDropProfile) Number of static signatutre violations dropped by the Bot profile.

Static Signature Redirect (staticSignnatureRedirectProfile) Number of static signatutre violations redirected by the Bot profile to a different Web page or web server.

Static Signature Reset (staticSignnatureResetProfile) Number of static signatutre violations reset by the Bot profile to a different Web page or web server.

TPS (tpsProfile) Number of tps violations seen by the Bot profile.

Tps Logs (tpsLogProfile) Number of tps violations logged by the Bot profile.

Tps Drop (tpsDropProfile) Number of tps violations dropped by the Bot profile.

Tps Redirect (tpsRedirectProfile) Number of tps violations requests redirected by the Bot profile to a different Web page or web server.

Tps Reset (tpsResetProfile) Number of tps violations reset by the Bot profile.

Tps Captcha (tpsCaptchaProfile) Number of tps violation requests for which CAPTCHA challenge was sent due to Bot profile.

Captcha (captchaProfile) Number of Captcha challenge failures seen by the Bot profile.

Captcha Log (captchaLogProfile) Number of Captcha challenge failures logged by the Bot profile.

Captcha Drop (captchaDropProfile) Number of Captcha challenge failures dropped by the Bot profile.

Captcha Redirect (captchaRedirectProfile) Number of Captcha challenge failures redirected by the Bot profile.

Captcha Reset (captchaResetProfile) Number of Captcha challenge failures reset by the Bot profile.

Trap (trapProfile) Number of trap violations seen by the Bot profile.

Trap Logs (trapLogProfile) Number of trap violations logged by the Bot profile.

Trap Drop (trapDropProfile) Number of trap violations dropped by the Bot profile.

Trap Redirect (trapRedirectProfile) Number of trap violations requests redirected by the Bot profile to a different Web page or web server.

Trap Reset (trapResetProfile) Number of trap violations reset by the Bot profile.

Bot whitelist enabled (botCfgWhitelistProfile) Whitelist enabled under bot profile.

Bot blacklist enabled (botCfgBlacklistProfile) Blacklist enabled under bot profile.

Bot IP Reputation enabled (botCfgIpRepProfile) IP Reputation enabled under bot profile.

Bot Ratelimit enabled (botCfgRatelimitProfile) Ratelimit enabled under bot profile.

Bot Signatures enabled (botCfgSignatureProfile) Static Signatures enabled under bot profile.

Bot device fingerprint enabled (botCfgDFPProfile) Device Fingerprint enabled under bot profile.

Bot TPS enabled (botCfgTpsProfile) TPS enabled under bot profile.

Bot Trap enabled (botCfgTrapProfile) Bot Trap enabled under bot profile.

Keyboard Mouse Detection enabled (botCfgKMDetectionProfile) Keyboard mouse detection enabled under bot profile.

Example

stat bot profile

Related Commands

- stat bot policylabel

bind bot profile

Bind the specified bot detection mechanism to the specified profile.

Synopsis

bind bot profile <name> ((-blackList -type <type> -value <string> -action <action> ...) | (-whiteList -type <type> -value <string>) | (-rateLimit -type <type> -rate <positive_integer> -timeSlice <positive_integer>) | (-ipReputation -category <category>) | (-captchaResource -url <string> -action <action> ...) | (-tps -type <type>) | (-trapInsertionURL -url <string>) | (-logExpression -name <string> -expression <expression>) | (-KMDetectionExpr -name <string> -expression <expression>))

Arguments

name Name for the profile. Must begin with a letter, number, or the underscore character (*), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at (@), equals (=), colon (:), and underscore (*) characters. Cannot be changed after the profile is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

blackList Blacklist binding. Maximum 32 bindings can be configured per profile for Blacklist detection.

type Type of the black-list entry.

Possible values: IPv4, SUBNET, IPv6, IPv6_SUBNET, EXPRESSION

value Value of the bot black-list entry.

action One or more actions to be taken if bot is detected based on this Blacklist binding. Only LOG action can be combined with DROP or RESET action. Default value: NONE

enabled Enabled or disbaled black-list binding.

Possible values: ON, OFF Default value: OFF

whiteList Whitelist binding. Maximum 32 bindings can be configured per profile for Whitelist detection.

type Type of the white-list entry.

Possible values: IPv4, SUBNET, IPv6, IPv6_SUBNET, EXPRESSION

value Value of bot white-list entry.

log Enable logging for Whitelist binding.

Possible values: ON, OFF Default value: OFF

enabled Enabled or disabled white-list binding.

Possible values: ON, OFF Default value: OFF

rateLimit Rate-limit binding. Maximum 30 bindings can be configured per profile for rate-limit detection. For SOURCE_IP type, only one binding can be configured, and for URL type, only one

binding is allowed per URL, and for SESSION type, only one binding is allowed for a cookie name. To update the values of an existing binding, user has to first unbind that binding, and then needs to bind again with new values.

type Rate-limiting type Following rate-limiting types are allowed: *SOURCE_IP - Rate-limiting based on the client IP. *SESSION - Rate-limiting based on the configured cookie name. *URL - Rate-limiting based on the configured URL. *GEOLOCATION - Rate-limiting based on the configured country name.

Possible values: SESSION, SOURCE_IP, URL, GEOLOCATION, JA3_FINGERPRINT

url URL for the resource based rate-limiting.

cookieName Cookie name which is used to identify the session for session rate-limiting.

countryCode Country name which is used for geolocation rate-limiting.

Possible values: AF, AX, AL, DZ, AS, AD, AO, AI, AQ, AG, AR, AM, AW, AU, AT, AZ, BS, BH, BD, BB, BY, BE, BZ, BJ, BM, BT, BO, BQ, BA, BW, BR, IO, BN, BG, BF, BI, KH, CM, CA, CV, KY, CF, TD, CL, CN, CX, CC, CO, KM, CG, CD, CK, CR, CI, HR, CU, CW, CY, CZ, DK, DJ, DM, DO, EC, EG, SV, GQ, ER, EE, ET, FK, FO, FJ, FI, FR, GF, PF, TF, GA, GM, GE, DE, GH, GI, GR, GL, GD, GP, GU, GT, GG, GN, GW, GY, HT, HM, VA, HN, HK, HU, IS, IN, ID, IR, IQ, IE, IM, IL, IT, JM, JP, JE, JO, KZ, KE, KI, XK, KW, KG, LA, LV, LB, LS, LR, LY, LI, LT, LU, MO, MK, MG, MW, MY, MV, ML, MT, MH, MQ, MR, MU, YT, MX, FM, MD, MC, MN, ME, MS, MA, MZ, MM, NA, NR, NP, NL, NC, NZ, NI, NE, NG, NU, NF, KP, MP, NO, OM, PK, PW, PS, PA, PG, PY, PE, PH, PN, PL, PT, PR, QA, RE, RO, RU, RW, BL, SH, KN, LC, MF, PM, VC, WS, SM, ST, SA, SN, RS, SC, SL, SG, SX, SK, SI, SB, SO, SZA, GS, KR, SS, ES, LK, SD, SR, SJ, SZ, SE, CH, SY, TW, TJ, TZ, TH, TL, TG, TK, TO, TT, TN, TR, TM, TC, TV, UG, UA, AE, GB, US, UM, UY, UZ, VU, VE, VN, VG, VI, WF, EH, YE, ZM, ZW

rate Maximum number of requests that are allowed in this session in the given period time. Default value: 1 Minimum value: 1

timeSlice Time interval during which requests are tracked to check if they cross the given rate. Default value: 1000 Minimum value: 10

limitType Rate-Limiting traffic Type

Possible values: BURSTY, SMOOTH Default value: BURSTY

condition Expression to be used in a rate-limiting condition. This expression result must be a boolean value.

action One or more actions to be taken when the current rate becomes more than the configured rate. Only LOG action can be combined with DROP, REDIRECT or RESET action. Default value: NONE

enabled Enable or disable rate-limit binding.

Possible values: ON, OFF Default value: OFF

ipReputation IP reputation binding. For each category, only one binding is allowed. To update the values of an existing binding, user has to first unbind that binding, and then needs to bind again with the new values.

category IP Repuation category. Following IP Reuputation categories are allowed: *IP_BASED - This category checks whether client IP is malicious or not. *BOTNET - This category includes Botnet C&C channels, and infected zombie machines controlled by Bot master. *SPAM_SOURCES - This category includes tunneling spam messages through a proxy, anomalous SMTP activities, and forum spam activities. *SCANNERS - This category includes all reconnaissance such as probes, host scan, domain scan, and password brute force attack. *DOS - This category includes DOS, DDOS, anomalous sync flood, and anomalous traffic detection. *REPUTATION - This category denies access from IP addresses currently known to be infected with malware. This category also includes IPs with average low Webroot Reputation Index score. Enabling this category will prevent access from sources identified to contact malware distribution points. *PHISHING - This category includes IP addresses hosting phishing sites and other kinds of fraud activities such as ad click fraud or gaming fraud. *PROXY - This category includes IP addresses providing proxy services. *NETWORK - IPs providing proxy and anonymization services including The Onion Router aka TOR or darknet. *MOBILE_THREATS - This category checks client IP with the list of IPs harmful for mobile devices. *WINDOWS_EXPLOITS - This category includes active IP address offering or distributig malware, shell code, rootkits, worms or viruses. *WEB_ATTACKS - This category includes cross site scripting, iFrame injection, SQL injection, cross domain injection or domain password brute force attack. *TOR_PROXY - This category includes IP address acting as exit nodes for the Tor Network. *CLOUD - This category checks client IP with list of public cloud IPs. *CLOUD_AWS - This category checks client IP with list of public cloud IPs from Amazon Web Services. *CLOUD_GCP - This category checks client IP with list of public cloud IPs from Google Cloud Platform. *CLOUD_AZURE - This category checks client IP with list of public cloud IPs from Azure. *CLOUD_ORACLE - This category checks client IP with list of public cloud IPs from Oracle. *CLOUD_IBM - This category checks client IP with list of public cloud IPs from IBM. *CLOUD_SALESFORCE - This category checks client IP with list of public cloud IPs from Salesforce.

Possible values: IP, BOTNETS, SPAM_SOURCES, SCANNERS, DOS, REPUTATION, PHISHING, PROXY, NETWORK, MOBILE_THREATS, WINDOWS_EXPLOITS, WEB_ATTACKS, TOR_PROXY, CLOUD, CLOUD_AWS, CLOUD_GCP, CLOUD_AZURE, CLOUD_ORACLE, CLOUD_IBM, CLOUD_SALESFORCE

enabled Enabled or disabled IP-repuation binding.

Possible values: ON, OFF Default value: OFF

action One or more actions to be taken if bot is detected based on this IP Reputation binding. Only LOG action can be combinded with DROP, RESET, REDIRECT or MITIGATION action. Default value: NONE

captchaResource Captcha action binding. For each URL, only one binding is allowed. To update the values of an existing URL binding, user has to first unbind that binding, and then needs to bind the URL again with new values. Maximum 30 bindings can be configured per profile.

url URL for which the Captcha action, if configured under IP reputation, TPS or device fingerprint, need to be applied.

waitTime Wait time in seconds for which ADC needs to wait for the Captcha response. This is to avoid DOS attacks. Default value: 15 Minimum value: 10 Maximum value: 60

gracePeriod Time (in seconds) duration for which no new captcha challenge is sent after current captcha challenge has been answered successfully. Default value: 900 Minimum value: 60 Maximum value: 900

mutePeriod Time (in seconds) duration for which client which failed captcha need to wait until allowed to try again. The requests from this client are silently dropped during the mute period. Default value: 300 Minimum value: 60 Maximum value: 900

requestSizeLimit Length of body request (in Bytes) up to (equal or less than) which captcha challenge will be provided to client. Above this length threshold the request will be dropped. This is to avoid DOS and DDOS attacks. Default value: 8000 Minimum value: 10 Maximum value: 30000

retryAttempts Number of times client can retry solving the captcha. Default value: 3 Minimum value: 1 Maximum value: 10

action One or more actions to be taken when client fails captcha challenge. Only, log action can be configured with DROP, REDIRECT or RESET action. Default value: NONE

enabled Enable or disable the captcha binding.

Possible values: ON, OFF Default value: OFF

tps TPS binding. For each type only binding can be configured. To update the values of an existing binding, user has to first unbind that binding, and then needs to bind again with new values.

type Type of TPS binding.

Possible values: SOURCE_IP, GEOLOCATION, REQUEST_URL, Host

threshold Maximum number of requests that are allowed from (or to) a IP, Geolocation, URL or Host in 1 second time interval. Minimum value: 1

percentage Maximum percentage increase in the requests from (or to) a IP, Geolocation, URL or Host in 30 minutes interval. Minimum value: 10

action One to more actions to be taken if bot is detected based on this TPS binding. Only LOG action can be combined with DROP, RESET, REDIRECT, or MITIGIATION action. Default value: NONE

enabled Enabled or disabled TPS binding.

Possible values: ON, OFF Default value: ON

trapInsertionURL Bind the trap URL for the configured request URLs. Maximum 30 bindings can be configured per profile.

url Request URL regex pattern for which Trap URL is inserted.

enabled Enable or disable the request URL pattern.

Possible values: ON, OFF Default value: OFF

logExpression Log expression binding.

name Name of the log expression object.

expression Expression whose result to be logged when violation happened on the bot profile.

enabled Enable or disable the log expression binding.

Possible values: ON, OFF Default value: OFF

KMDetectionExpr Keyboard-mouse based detection binding. For each name, only one binding is allowed. To update the values of an existing binding, user has to first unbind that binding, then needs to bind again with new vlaues. Maximum 30 bindings can be configured per profile.

name Name of the keyboard-mouse expression object.

expression JavaScript file for keyboard-mouse detection, would be inserted if the result of the expression is true.

enabled Enable or disable the keyboard-mouse based binding.

Possible values: ON, OFF Default value: OFF

logMessage Message to be logged for this binding.

comment Any comments about this binding.

set bot profile

Set the bot profile parameters

Synopsis

set bot profile <name>

Arguments

name Name for the profile. Must begin with a letter, number, or the underscore character (*), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at (@), equals (=), colon (:), and underscore (*) characters. Cannot be changed after the profile is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

signature Name of object containing bot static signature details.

errorURL URL that Bot protection uses as the Error URL. Default value: NS_S_BOT_DEFAULT_ERRORURL

trapURL URL that Bot protection uses as the Trap URL. Default value: NS_S_BOT_DEFAULT_TRAPURL

comment Any comments about the purpose of profile, or other useful information about the profile. Default value: NS_S_BOT_DEFAULT_PROFILE_COMMENTS

whiteList Enable white-list bot detection.

Possible values: ON, OFF Default value: OFF

blackList Enable black-list bot detection.

Possible values: ON, OFF Default value: OFF

rateLimit Enable rate-limit bot detection.

Possible values: ON, OFF Default value: OFF

deviceFingerprint Enable device-fingerprint bot detection

Possible values: ON, OFF Default value: OFF

deviceFingerprintAction Action to be taken for device-fingerprint based bot detection. Default value: NONE

ipReputation Enable IP-reputation bot detection.

Possible values: ON, OFF Default value: OFF

trap Enable trap bot detection.

Possible values: ON, OFF Default value: OFF

signatureNoUserAgentHeaderAction Actions to be taken if no User-Agent header in the request (Applicable if Signature check is enabled). Default value: DROP

signatureMultipleUserAgentHeaderAction Actions to be taken if multiple User-Agent headers are seen in a request (Applicable if Signature check is enabled). Log action should be combined with other actions Default value: CHECKLAST

trapAction Action to be taken for bot trap based bot detection. Default value: NONE

tps Enable TPS.

Possible values: ON, OFF Default value: OFF

deviceFingerprintMobile Enabling bot device fingerprint protection for mobile clients Default value: NONE

headlessBrowserDetection Enable Headless Browser detection.

Possible values: ON, OFF Default value: OFF

clientIpExpression Expression to get the client IP.

KMJavaScriptName Name of the JavaScript file that the Bot Management feature will insert in the response for keyboard-mouse based detection. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my javascript file name" or 'my javascript file name'). Default value: NS_S_BOT_DEFAULT_KM_JS_NAME

KMDetection Enable keyboard-mouse based bot detection.

Possible values: ON, OFF Default value: OFF

KMEventsPostBodyLimit Size of the KM data send by the browser, needs to be processed on ADC Default value: NS_BOT_DEFAULT_KM_POST_BODY_LIMIT Minimum value: 1 Maximum value: 204800

verboseLogLevel Bot verbose Logging. Based on the log level, ADC will log additional information whenever client is detected as a bot.

Possible values: NONE, HTTP_FULL_HEADER Default value: NONE

spoofedReqAction Actions to be taken on a spoofed request (A request spoofing good bot user agent string). Default value: BOT_ACTION_LOG_DROP

dfpRequestLimit Number of requests to allow without bot session cookie if device fingerprint is enabled Minimum value: 1

sessionCookieName Name of the SessionCookie that the Bot Management feature uses for tracking. Must begin with a letter or number, and can consist of from 1 to 31 letters, numbers, and the hyphen (-) and underscore (_) symbols.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cookie name" or 'my cookie name').

sessionTimeout Timeout, in seconds, after which a user session is terminated. Minimum value: 1 Maximum value: 65535

show bot profile

Displays details of the specified bot profile. If no profile is specified, displays a list of all bot profiles on the Citrix ADC.

Synopsis

show bot profile

Arguments

name Name of the bot management profile.

Output

stateflag signature Name of object containing bot static signature details.

errorURL URL that Bot protection uses as the Error URL.

trapURL URL that Bot protection uses as the Trap URL.

comment Any comments about the purpose of profile, or other useful information about the profile.

builtin Flag to determine if bot profille is built-in or not

feature The feature to be checked while applying this config

whiteList Enable white-list bot detection.

blackList Enable black-list bot detection.

rateLimit Enable rate-limit bot detection.

deviceFingerprint Enable device-fingerprint bot detection

deviceFingerprintAction Action to be taken for device-fingerprint based bot detection.

ipReputation Enable IP-reputation bot detection.

trap Enable trap bot detection.

signatureNoUserAgentHeaderAction Actions to be taken if no User-Agent header in the request (Applicable if Signature check is enabled).

spoofedReqAction Actions to be taken on a spoofed request (A request spoofing good bot user agent string).

signatureMultipleUserAgentHeaderAction Actions to be taken if multiple User-Agent headers are seen in a request (Applicable if Signature check is enabled). Log action should be combined with other actions

trapAction Action to be taken for bot trap based bot detection.

tps Enable TPS.

blackList Blacklist binding. Maximum 32 bindings can be configured per profile for Blacklist detection.

whiteList Whitelist binding. Maximum 32 bindings can be configured per profile for Whitelist detection.

rateLimit Rate-limit binding. Maximum 30 bindings can be configured per profile for rate-limit detection. For SOURCE_IP type, only one binding can be configured, and for URL type, only one binding is allowed per URL, and for SESSION type, only one binding is allowed for a cookie name. To update the values of an existing binding, user has to first unbind that binding, and then needs to bind again with new values.

ipReputation IP reputation binding. For each category, only one binding is allowed. To update the values of an existing binding, user has to first unbind that binding, and then needs to bind again with the new values.

captchaResource Captcha action binding. For each URL, only one binding is allowed. To update the values of an existing URL binding, user has to first unbind that binding, and then needs to bind the URL again with new values. Maximum 30 bindings can be configured per profile.

tps TPS binding. For each type only binding can be configured. To update the values of an existing binding, user has to first unbind that binding, and then needs to bind again with new values.

type Type of the black-list entry.

type Type of the white-list entry.

enabled Enabled or disbaled black-list binding.

enabled Enabled or disabled white-list binding.

value Value of the bot black-list entry.

value Value of bot white-list entry.

action One or more actions to be taken if bot is detected based on this Blacklist binding. Only LOG action can be combined with DROP or RESET action.

type Type of TPS binding.

threshold Maximum number of requests that are allowed from (or to) a IP, Geolocation, URL or Host in 1 second time interval.

percentage Maximum percentage increase in the requests from (or to) a IP, Geolocation, URL or Host in 30 minutes interval.

action One to more actions to be taken if bot is detected based on this TPS binding. Only LOG action can be combined with DROP, RESET, REDIRECT, or MITIGIATION action.

enabled Enabled or disabled TPS binding.

category IP Repuation category. Following IP Reuputation categories are allowed: *IP_BASED - This category checks whether client IP is malicious or not. *BOTNET - This category includes Botnet C&C channels, and infected zombie machines controlled by Bot master. *SPAM_SOURCES - This category includes tunneling spam messages through a proxy, anomalous SMTP activities, and forum spam activities. *SCANNERS - This category includes all reconnaissance such as probes, host scan, domain scan, and password brute force attack. *DOS - This category includes DOS, DDOS, anomalous sync flood, and anomalous traffic detection. *REPUTATION - This category denies access from IP addresses currently known to be infected with malware. This category also includes IPs with average low Webroot Reputation Index score. Enabling this category will prevent access from sources identified to contact malware distribution points. *PHISHING - This category includes IP addresses hosting phishing sites and other kinds of fraud activities such as ad click fraud or gaming fraud. *PROXY - This category includes IP addresses providing proxy services. *NETWORK - IPs providing proxy and anonymization services including The Onion Router aka TOR or darknet. *MOBILE_THREATS - This category checks client IP with the list of IPs harmful for mobile devices. *WINDOWS_EXPLOITS - This category includes active IP address offering or distributig malware, shell code, rootkits, worms or viruses. *WEB_ATTACKS - This category includes cross site scripting, iFrame injection, SQL injection, cross domain injection or domain password brute force attack. *TOR_PROXY - This category includes IP address acting as exit nodes for the Tor Network. *CLOUD - This category checks client IP with list of public cloud IPs. *CLOUD_AWS - This category checks client IP with list of public cloud IPs from Amazon Web Services. *CLOUD_GCP - This category checks client IP with list of public cloud IPs from Google Cloud Platform. *CLOUD_AZURE - This category checks client IP with list of public cloud IPs from Azure. *CLOUD_ORACLE - This category checks client IP with list of public cloud IPs from Oracle. *CLOUD_IBM - This category checks client IP with list of public cloud IPs from IBM. *CLOUD_SALESFORCE - This category checks client IP with list of public cloud IPs from Salesforce.

action One or more actions to be taken if bot is detected based on this IP Reputation binding. Only LOG action can be combinded with DROP, RESET, REDIRECT or MITIGATION action.

enabled Enabled or disabled IP-repuation binding.

type Rate-limiting type Following rate-limiting types are allowed: *SOURCE_IP - Rate-limiting based on the client IP. *SESSION - Rate-limiting based on the configured cookie name. *URL - Rate-limiting based on the configured URL. *GEOLOCATION - Rate-limiting based on the configured country name.

url URL for the resource based rate-limiting.

cookieName Cookie name which is used to identify the session for session rate-limiting.

rate Maximum number of requests that are allowed in this session in the given period time.

limitType Rate-Limiting traffic Type

condition Expression to be used in a rate-limiting condition. This expression result must be a boolean value.

timeSlice Time interval during which requests are tracked to check if they cross the given rate.

action One or more actions to be taken when the current rate becomes more than the configured rate. Only LOG action can be combined with DROP, REDIRECT or RESET action.

enabled Enable or disable rate-limit binding.

url URL for which the Captcha action, if configured under IP reputation, TPS or device fingerprint, need to be applied.

waitTime Wait time in seconds for which ADC needs to wait for the Captcha response. This is to avoid DOS attacks.

gracePeriod Time (in seconds) duration for which no new captcha challenge is sent after current captcha challenge has been answered successfully.

mutePeriod Time (in seconds) duration for which client which failed captcha need to wait until allowed to try again. The requests from this client are silently dropped during the mute period.

requestSizeLimit Length of body request (in Bytes) up to (equal or less than) which captcha challenge will be provided to client. Above this length threshold the request will be dropped. This is to avoid DOS and DDOS attacks.

retryAttempts Number of times client can retry solving the captcha.

action One or more actions to be taken when client fails captcha challenge. Only, log action can be configured with DROP, REDIRECT or RESET action.

enabled Enable or disable the captcha binding.

log Enable logging for Whitelist binding.

logMessage Message to be logged for this binding.

comment Any comments about this binding.

trapInsertionURL Bind the trap URL for the configured request URLs. Maximum 30 bindings can be configured per profile.

url Request URL regex pattern for which Trap URL is inserted.

enabled Enable or disable the request URL pattern.

deviceFingerprintMobile Enabling bot device fingerprint protection for mobile clients

headlessBrowserDetection Enable Headless Browser detection.

logExpression Log expression binding.

name Name of the log expression object.

expression Expression whose result to be logged when violation happened on the bot profile.

enabled Enable or disable the log expression binding.

clientIpExpression Expression to get the client IP.

KMJavaScriptName Name of the JavaScript file that the Bot Management feature will insert in the response for keyboard-mouse based detection. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my javascript file name" or 'my javascript file name').

KMDetection Enable keyboard-mouse based bot detection.

KMDetectionExpr Keyboard-mouse based detection binding. For each name, only one binding is allowed. To update the values of an existing binding, user has to first unbind that binding, then needs to bind again with new vlaues. Maximum 30 bindings can be configured per profile.

enabled Enable or disable the keyboard-mouse based binding.

name Name of the keyboard-mouse expression object.

expression JavaScript file for keyboard-mouse detection, would be inserted if the result of the expression is true.

KMEventsPostBodyLimit Size of the KM data send by the browser, needs to be processed on ADC

verboseLogLevel Bot verbose Logging. Based on the log level, ADC will log additional information whenever client is detected as a bot.

countryCode Country name which is used for geolocation rate-limiting.

dfpRequestLimit Number of requests to allow without bot session cookie if device fingerprint is enabled

sessionCookieName Name of the SessionCookie that the Bot Management feature uses for tracking. Must begin with a letter or number, and can consist of from 1 to 31 letters, numbers, and the hyphen (-) and underscore (_) symbols.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cookie name" or 'my cookie name').

sessionTimeout Timeout, in seconds, after which a user session is terminated.

devno count

add bot profile

Creates bot profile, which has configuration options for bot management. (A profile is equivalent to an action in other Citrix ADC features.)

Synopsis

add bot profile <name>

Arguments

name Name for the profile. Must begin with a letter, number, or the underscore character (*), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at (@), equals (=), colon (:), and underscore (*) characters. Cannot be changed after the profile is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

signature Name of object containing bot static signature details.

errorURL URL that Bot protection uses as the Error URL. Default value: NS_S_BOT_DEFAULT_ERRORURL

trapURL URL that Bot protection uses as the Trap URL. Default value: NS_S_BOT_DEFAULT_TRAPURL

comment Any comments about the purpose of profile, or other useful information about the profile. Default value: NS_S_BOT_DEFAULT_PROFILE_COMMENTS

whiteList Enable white-list bot detection.

Possible values: ON, OFF Default value: OFF

blackList Enable black-list bot detection.

Possible values: ON, OFF Default value: OFF

rateLimit Enable rate-limit bot detection.

Possible values: ON, OFF Default value: OFF

deviceFingerprint Enable device-fingerprint bot detection

Possible values: ON, OFF Default value: OFF

deviceFingerprintAction Action to be taken for device-fingerprint based bot detection. Default value: NONE

ipReputation Enable IP-reputation bot detection.

Possible values: ON, OFF Default value: OFF

trap Enable trap bot detection.

Possible values: ON, OFF Default value: OFF

trapAction Action to be taken for bot trap based bot detection. Default value: NONE

signatureNoUserAgentHeaderAction Actions to be taken if no User-Agent header in the request (Applicable if Signature check is enabled). Default value: DROP

signatureMultipleUserAgentHeaderAction Actions to be taken if multiple User-Agent headers are seen in a request (Applicable if Signature check is enabled). Log action should be combined with other actions Default value: CHECKLAST

tps Enable TPS.

Possible values: ON, OFF Default value: OFF

deviceFingerprintMobile Enabling bot device fingerprint protection for mobile clients Default value: NONE

headlessBrowserDetection Enable Headless Browser detection.

Possible values: ON, OFF Default value: OFF

clientIpExpression Expression to get the client IP.

KMJavaScriptName Name of the JavaScript file that the Bot Management feature will insert in the response for keyboard-mouse based detection. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my javascript file name" or 'my javascript file name'). Default value: NS_S_BOT_DEFAULT_KM_JS_NAME

KMDetection Enable keyboard-mouse based bot detection.

Possible values: ON, OFF Default value: OFF

KMEventsPostBodyLimit Size of the KM data send by the browser, needs to be processed on ADC Default value: NS_BOT_DEFAULT_KM_POST_BODY_LIMIT Minimum value: 1 Maximum value: 204800

verboseLogLevel Bot verbose Logging. Based on the log level, ADC will log additional information whenever client is detected as a bot.

Possible values: NONE, HTTP_FULL_HEADER Default value: NONE

spoofedReqAction Actions to be taken on a spoofed request (A request spoofing good bot user agent string). Default value: BOT_ACTION_LOG_DROP

dfpRequestLimit Number of requests to allow without bot session cookie if device fingerprint is enabled Minimum value: 1

sessionCookieName Name of the SessionCookie that the Bot Management feature uses for tracking. Must begin with a letter or number, and can consist of from 1 to 31 letters, numbers, and the hyphen (-) and underscore (_) symbols.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cookie name" or 'my cookie name').

sessionTimeout Timeout, in seconds, after which a user session is terminated. Minimum value: 1 Maximum value: 65535

unbind bot profile

Unbind the specified bot detection mechanism to the specified profile.

Synopsis

unbind bot profile <name> ((-blackList -value <string>) | (-whiteList -value <string>) | (-rateLimit -type <type>) | (-ipReputation -category <category>) | (-captchaResource -url <string>) | (-tps -type <type>) | (-trapInsertionURL -url <string>) | (-logExpression -name <string>) | (-KMDetectionExpr -name <string>))

Arguments

name Name for the profile. Must begin with a letter, number, or the underscore character (*), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at (@), equals (=), colon (:), and underscore (*) characters. Cannot be changed after the profile is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

blackList Blacklist binding. Maximum 32 bindings can be configured per profile for Blacklist detection.

value Value of the bot black-list entry.

whiteList Whitelist binding. Maximum 32 bindings can be configured per profile for Whitelist detection.

value Value of bot white-list entry.

rateLimit Rate-limit binding. Maximum 30 bindings can be configured per profile for rate-limit detection. For SOURCE_IP type, only one binding can be configured, and for URL type, only one binding is allowed per URL, and for SESSION type, only one binding is allowed for a cookie name. To update the values of an existing binding, user has to first unbind that binding, and then needs to bind again with new values.

type Rate-limiting type Following rate-limiting types are allowed: *SOURCE_IP - Rate-limiting based on the client IP. *SESSION - Rate-limiting based on the configured cookie name. *URL - Rate-limiting based on the configured URL. *GEOLOCATION - Rate-limiting based on the configured country name.

Possible values: SESSION, SOURCE_IP, URL, GEOLOCATION, JA3_FINGERPRINT

url URL for the resource based rate-limiting.

cookieName Cookie name which is used to identify the session for session rate-limiting.

countryCode Country name which is used for geolocation rate-limiting.

Possible values: AF, AX, AL, DZ, AS, AD, AO, AI, AQ, AG, AR, AM, AW, AU, AT, AZ, BS, BH, BD, BB, BY, BE, BZ, BJ, BM, BT, BO, BQ, BA, BW, BR, IO, BN, BG, BF, BI, KH, CM, CA, CV, KY, CF, TD, CL, CN, CX, CC, CO, KM, CG, CD, CK, CR, CI, HR, CU, CW, CY, CZ, DK, DJ, DM, DO, EC, EG, SV, GQ, ER, EE, ET, FK, FO, FJ, FI, FR, GF, PF, TF, GA, GM, GE, DE, GH, GI, GR, GL, GD, GP, GU, GT, GG, GN, GW, GY, HT, HM, VA, HN, HK, HU, IS, IN, ID, IR, IQ, IE, IM, IL, IT, JM, JP, JE, JO, KZ, KE, KI, XK, KW, KG, LA, LV, LB, LS, LR, LY, LI, LT, LU, MO, MK, MG, MW, MY, MV, ML, MT, MH, MQ, MR, MU, YT, MX, FM, MD, MC, MN, ME, MS, MA, MZ, MM, NA, NR, NP, NL, NC, NZ, NI, NE, NG, NU, NF, KP, MP, NO, OM, PK, PW, PS, PA, PG, PY, PE, PH, PN, PL, PT, PR, QA, RE, RO, RU, RW, BL, SH, KN, LC, MF, PM, VC, WS, SM, ST, SA, SN, RS, SC, SL, SG, SX, SK, SI, SB, SO, SZA, GS, KR, SS, ES, LK, SD, SR, SJ, SZ, SE, CH, SY, TW, TJ, TZ, TH, TL, TG, TK, TO, TT, TN, TR, TM, TC, TV, UG, UA, AE, GB, US, UM, UY, UZ, VU, VE, VN, VG, VI, WF, EH, YE, ZM, ZW

condition Expression to be used in a rate-limiting condition. This expression result must be a boolean value.

ipReputation IP reputation binding. For each category, only one binding is allowed. To update the values of an existing binding, user has to first unbind that binding, and then needs to bind again with the new values.

category IP Repuation category. Following IP Reuputation categories are allowed: *IP_BASED - This category checks whether client IP is malicious or not. *BOTNET - This category includes Botnet C&C channels, and infected zombie machines controlled by Bot master. *SPAM_SOURCES - This category includes tunneling spam messages through a proxy, anomalous SMTP activities, and forum spam activities. *SCANNERS - This category includes all reconnaissance such as probes, host scan, domain scan, and password brute force attack. *DOS - This category includes DOS, DDOS, anomalous sync flood, and anomalous traffic detection. *REPUTATION - This category denies access from IP addresses currently known to be infected with malware. This category also includes IPs with average low Webroot Reputation Index score. Enabling this category will prevent access from sources identified to contact malware distribution points. *PHISHING - This category includes IP addresses hosting phishing sites and other kinds of fraud activities such as ad click fraud or gaming fraud. *PROXY - This category includes IP addresses providing proxy services. *NETWORK - IPs providing proxy and anonymization services including The Onion Router aka TOR or darknet. *MOBILE_THREATS - This category checks client IP with the list of IPs harmful for mobile devices. *WINDOWS_EXPLOITS - This category includes active IP address offering or distributig malware, shell code, rootkits, worms or viruses. *WEB_ATTACKS - This category includes cross site scripting, iFrame injection, SQL injection, cross domain injection or domain password brute force attack. *TOR_PROXY - This category includes IP address acting as exit nodes for the Tor Network. *CLOUD - This category checks client IP with list of public cloud IPs. *CLOUD_AWS - This category checks client IP with list of public cloud IPs from Amazon Web Services. *CLOUD_GCP - This category checks client IP with list of public cloud IPs from Google Cloud Platform. *CLOUD_AZURE - This category checks client IP with list of public cloud IPs from Azure. *CLOUD_ORACLE - This category checks client IP with list of public cloud IPs from Oracle. *CLOUD_IBM - This category checks client IP with list of public cloud IPs from IBM. *CLOUD_SALESFORCE - This category checks client IP with list of public cloud IPs from Salesforce.

Possible values: IP, BOTNETS, SPAM_SOURCES, SCANNERS, DOS, REPUTATION, PHISHING, PROXY, NETWORK, MOBILE_THREATS, WINDOWS_EXPLOITS, WEB_ATTACKS, TOR_PROXY, CLOUD, CLOUD_AWS, CLOUD_GCP, CLOUD_AZURE, CLOUD_ORACLE, CLOUD_IBM, CLOUD_SALESFORCE

captchaResource Captcha action binding. For each URL, only one binding is allowed. To update the values of an existing URL binding, user has to first unbind that binding, and then needs to bind the URL again with new values. Maximum 30 bindings can be configured per profile.

url URL for which the Captcha action, if configured under IP reputation, TPS or device fingerprint, need to be applied.

tps TPS binding. For each type only binding can be configured. To update the values of an existing binding, user has to first unbind that binding, and then needs to bind again with new values.

type Type of TPS binding.

Possible values: SOURCE_IP, GEOLOCATION, REQUEST_URL, Host

trapInsertionURL Bind the trap URL for the configured request URLs. Maximum 30 bindings can be configured per profile.

url Request URL regex pattern for which Trap URL is inserted.

logExpression Log expression binding.

name Name of the log expression object.

KMDetectionExpr Keyboard-mouse based detection binding. For each name, only one binding is allowed. To update the values of an existing binding, user has to first unbind that binding, then needs to bind again with new vlaues. Maximum 30 bindings can be configured per profile.

name Name of the keyboard-mouse expression object.

rm bot profile

Removes the specified bot management profile.

Synopsis

rm bot profile <name>

Arguments

name Name of the profile.

bot-settings

The following operations can be performed on "bot-settings":

show| unset| set|

show bot settings

Displays the current Bot Management global settings.

Synopsis

show bot settings

Arguments

Output

defaultProfile Profile to use when a connection does not match any policy. Default setting is " ", which sends unmatched connections back to the Citrix ADC without attempting to filter them further.

defaultNonIntrusiveProfile Profile to use when the feature is not enabled but feature is licensed. NonIntrusive checks will be disabled and IPRep cronjob(24 Hours) will be removed if this is set to BOT_BYPASS.

javaScriptName Name of the JavaScript that the Bot Management feature uses in response. Must begin with a letter or number, and can consist of from 1 to 31 letters, numbers, and the hyphen (-) and underscore (_) symbols.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cookie name" or 'my cookie name').

sessionTimeout Timeout, in seconds, after which a user session is terminated.

sessionCookieName Name of the SessionCookie that the Bot Management feature uses for tracking. Must begin with a letter or number, and can consist of from 1 to 31 letters, numbers, and the hyphen (-) and underscore (_) symbols.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cookie name" or 'my cookie name').

dfpRequestLimit Number of requests to allow without bot session cookie if device fingerprint is enabled

signatureAutoUpdate Flag used to enable/disable bot auto update signatures

signatureUrl URL to download the bot signature mapping file from server

proxyServer Proxy Server IP to get updated signatures from AWS.

proxyPort Proxy Server Port to get updated signatures from AWS.

proxyUsername Proxy Username

proxyPassword Password with which user logs on.

trapURLAutoGenerate Enable/disable trap URL auto generation. When enabled, trap URL is updated within the configured interval.

trapURLInterval Time in seconds after which trap URL is updated.

trapURLLength Length of the auto-generated trap URL.

builtin Flag to determine if bot engine setting is built-in or not

feature The feature to be checked while applying this config

unset bot settings

Use this command to remove bot settings settings.Refer to the set bot settings command for meanings of the arguments.

Synopsis

unset bot settings

set bot settings

Modifies the global bot settings. The global settings apply to all bot profiles.

Synopsis

set bot settings [-proxyUsername <string>]

Arguments

defaultProfile Profile to use when a connection does not match any policy. Default setting is " ", which sends unmatched connections back to the Citrix ADC without attempting to filter them further. Default value: NS_S_BOT_DEFAULT_PROFILE

defaultNonIntrusiveProfile Profile to use when the feature is not enabled but feature is licensed. NonIntrusive checks will be disabled and IPRep cronjob(24 Hours) will be removed if this is set to BOT_BYPASS.

Possible values: BOT_BYPASS, BOT_STATS, BOT_LOG Default value: BOT_STATS Minimum value: 1

javaScriptName Name of the JavaScript that the Bot Management feature uses in response. Must begin with a letter or number, and can consist of from 1 to 31 letters, numbers, and the hyphen (-) and underscore (_) symbols.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cookie name" or 'my cookie name'). Default value: NS_S_BOT_DEFAULT_JS_NAME

sessionTimeout Timeout, in seconds, after which a user session is terminated. Default value: NS_BOT_DEFAULT_SESSION_TIMEOUT Minimum value: 1 Maximum value: 65535

sessionCookieName Name of the SessionCookie that the Bot Management feature uses for tracking. Must begin with a letter or number, and can consist of from 1 to 31 letters, numbers, and the hyphen (-) and underscore (_) symbols.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cookie name" or 'my cookie name'). Default value: NS_S_BOT_DEFAULT_SESSION_CKI_NAME

dfpRequestLimit Number of requests to allow without bot session cookie if device fingerprint is enabled Default value: NS_BOT_DEFAULT_DFP_REQUEST_LIMIT Minimum value: 1

signatureAutoUpdate Flag used to enable/disable bot auto update signatures

Possible values: ON, OFF Default value: OFF

signatureUrl URL to download the bot signature mapping file from server Default value: https://nsbotsignatures.s3.amazonaws.com/BotSignatureMapping.json

proxyServer Proxy Server IP to get updated signatures from AWS.

proxyPort Proxy Server Port to get updated signatures from AWS. Default value: 8080

trapURLAutoGenerate Enable/disable trap URL auto generation. When enabled, trap URL is updated within the configured interval.

Possible values: ON, OFF Default value: OFF

trapURLInterval Time in seconds after which trap URL is updated. Default value: 3600 Minimum value: 300 Maximum value: 86400

trapURLLength Length of the auto-generated trap URL. Default value: 32 Minimum value: 10 Maximum value: 255

proxyUsername Proxy Username

proxyPassword Password with which user logs on.

bot-signature

The following operations can be performed on "bot-signature":

rm| show| update| import|

rm bot signature

Removes the specified signature object.

Synopsis

rm bot signature <name>

Arguments

name Name to assign to the bot signature file object on the Citrix ADC.

Example

rm bot signature <name>

show bot signature

Displays the specified signature object. If no signature object is specified, lists all bot signature objects on the Citrix ADC.

Synopsis

show bot signature

Arguments

name Name of the Bot signature object to display.

Output

response src Local path to and name of, or URL (protocol, host, path, and file name) for, the file in which to store the imported signature file. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

Example

show bot signature

update bot signature

Updates the specified signature object from the source.

Synopsis

update bot signature <name>

Arguments

name Name to assign to the bot signature file object on the Citrix ADC.

Example

update bot signature my-signature-data

import bot signature

Imports the specified Signature page to the Citrix ADC, assigns it the specified name, and stores it in the list of BOT signature objects.

Synopsis

import bot signature <name>

Arguments

src Local path to and name of, or URL (protocol, host, path, and file name) for, the file in which to store the imported signature file. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

name Name to assign to the bot signature file object on the Citrix ADC.

comment Any comments to preserve information about the signature file object.

overwrite Overwrites the existing file

Example

import bot signature http://www.example.com/page.json my-signature-data

bot-stats

The following operations can be performed on "bot-stats":

show bot stats

show bot stats is an alias for stat bot

Synopsis

show bot stats - alias for 'stat bot'

bot

The following operations can be performed on "bot":

stat bot

Displays bot statistics.

Synopsis

stat bot

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

requests (reqs) HTTP/HTTPS requests sent to your protected web servers via the Bot Management.

Request Bytes (reqBytes) Number of bytes transfered for requests

responses (resps) HTTP/HTTPS responses sent by your protected web servers via the Bot Management.

Response Bytes (resBytes) Number of bytes transfered for responses

total logs (botLog) Total number of logs by the bot management.

total drop (botDrop) Total number of drops by the bot management.

total redirect (botRedirect) Total number of redirects by the bot management.

total reset (botReset) Total number of resets by the bot management.

Device Fingerprint (deviceFingerPrint) Number of device fingerprint violations seen by the Bot Management.

Device Fingerprint Logs (deviceFingerPrintLog) Number of device fingerprint violations logged by the Bot Management.

Device Fingerprint Drop (deviceFingerPrintDrop) Number of device fingerprint violations dropped by the Bot Management.

Device Fingerprint Redirect (deviceFingerPrintRedirect) Number of device fingerprint violations requests redirected by the Bot Management to a different Web page or web server.

Device Fingerprint Captcha (deviceFingerPrintCaptcha) Number of device fingerprint violations requests for which CAPTCHA challenge was sent.

Device Fingerprint Reset (deviceFingerPrintReset) Number of device fingerprint violations reset by the Bot Management.

IP Reputation (ipRep) Number of ip reputation violations seen by the Bot Management.

IP Reputation Logs (ipRepLog) Number of ip reputation violations logged by the Bot Management.

IP Reputation Drop (ipRepDrop) Number of ip reputation violations dropped by the Bot Management.

IP Reputation Redirect (ipRepRedirect) Number of ip reputation violations requests redirected by the Bot Management to a different Web page or web server.

IP Reputation Captcha (ipRepCaptcha) Number of ip reputation violations requests for which CAPTCHA challenge was sent.

IP Reputation Reset (ipRepReset) Number of ip reputation violations reset by the Bot Management.

White List (whiteList) Number of white list violations seen by the Bot Management.

White List Logs (whiteListLog) Number of white list violations logged by the Bot Management.

Black List (blackList) Number of black list violations seen by the Bot Management.

Black List Logs (blackListLog) Number of black list violations logged by the Bot Management.

Black List Drop (blackListDrop) Number of black list violations dropped by the Bot Management.

Black List Reset (blackListReset) Number of black list violations reset by the Bot Management.

Black List Redirect (blackListRedirect) Number of black list violations redirected by the Bot Management to a different Web page or web server.

Rate Limit (rateLimit) Number of rate limiting violations seen by the Bot Management.

Rate Limit Logs (rateLimitLog) Number of rate limiting violations logged by the Bot Management.

Rate Limit Drop (rateLimitDrop) Number of rate limiting violations dropped by the Bot Management.

Rate Limit Redirect (rateLimitRedirect) Number of rate limiting violations requests redirected by the Bot Management to a different Web page or web server.

Rate Limit Reset (rateLimitReset) Number of rate limiting violations reset by the Bot Management.

Static Signature (staticSignature) Number of static signature violations seen by the Bot Management.

Static Signature Logs (staticSignatureLog) Number of static signature violations logged by the Bot Management.

Static Signature Drop (staticSignatureDrop) Number of static signature violations dropped by the Bot Management.

Static Signature Redirect (staticSignatureRediect) Number of static signature violations requests redirected by the Bot Management to a different Web page or web server.

Static Signature Reset (staticSignatureReset) Number of static signature violations requests reset by the Bot Management to a different Web page or web server.

Tps (tps) Number of tps violations seen by the Bot Management.

Tps Logs (tpsLog) Number of tps violations logged by the Bot Management.

Tps Drop (tpsDrop) Number of tps violations dropped by the Bot Management.

Tps Redirect (tpsRedirect) Number of tps violations requests redirected by the Bot Management to a different Web page or web server.

Tps Reset (tpsReset) Number of tps violations reset by the Bot Management.

Tps Captcha (tpsCaptcha) Number of TPS violations requests for which CAPTCHA challenge was sent.

Captcha (captcha) Number of Captcha challenge failures seen by the Bot Management.

Captcha Log (captchaLog) Number of Captcha challenge failures logged by the Bot Management.

Captcha Drop (captchaDrop) Number of Captcha challenge failures dropped by the Bot Management.

Captcha Redirect (captchaRedirect) Number of Captcha challenge failures redirected by the Bot Management.

Captcha Reset (captchaReset) Number of Captcha challenge failures reset by the Bot Management.

Trap (trap) Number of trap violations seen by the Bot Management.

Trap Logs (trapLog) Number of trap violations logged by the Bot Management.

Trap Drop (trapDrop) Number of trap violations dropped by the Bot Management.

Trap Redirect (trapRedirect) Number of trap violations requests redirected by the Bot Management to a different Web page or web server.

Trap Reset (trapReset) Number of trap violations reset by the Bot Management.

Profiles with WhiteList (botCfgWhitelist) Profiles with Whitelist enabled.

Profiles with BlackList (botCfgBlacklist) Profiles with Blacklist enabled.

Profiles with IP reputation (botCfgIpRep) Profiles with IP Reputation enabled.

Profiles with Ratelimit (botCfgRatelimit) Profiles with Ratelimit enabled.

Profiles with Signatures (botCfgSignature) Profiles with Static Signatures enabled.

Profiles with Device Fingerprint (botCfgDFP) Profiles with Device Fingerprint enabled.

Profiles with TPS (botCfgTps) Profiles with TPS enabled.

Profiles with Trap (botCfgTrap) Profiles with Bot Trap enabled.

Profiles with KM Detection (botCfgKMDetection) Profiles with Keyboard mouse detection enabled.

Related Commands

- stat bot policylabel

Botmgmt

The entities on which you can perform NetScaler CLI operations:

- bot
- bot-global
- bot-policy
- bot-policylabel
- bot-profile
- bot-settings
- bot-signature
- bot-stats

cache

Cache

The entities on which you can perform NetScaler CLI operations:

- cache
- cache-contentGroup
- cache-forwardProxy
- cache-global
- cache-object
- cache-parameter
- cache-policy
- cache-policylabel
- cache-selector
- cache-stats

cache-contentGroup

The following operations can be performed on "cache-contentGroup":

add| rm| save| flush| set| stat| expire| show| unset|

add cache contentGroup

Creates a new content group for grouping cached objects on the basis of some unique property.

Synopsis

add cache contentGroup <name> [(-hitParams <string> ...)] [-invalParams <string> ...] [-prefetch (YES | NO)]

Arguments

name Name for the content group. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the content group is created.

weakPosRelExpiry Relative expiry time, in seconds, for expiring positive responses with response codes between 200 and 399. Cannot be used in combination with other Expiry attributes. Similar to -relExpiry but has lower precedence. Default value: -1 Maximum value: 31536000

heurExpiryParam Heuristic expiry time, in percent of the duration, since the object was last modified. Default value: -1 Minimum value: 0 Maximum value: 100

relExpiry Relative expiry time, in seconds, after which to expire an object cached in this content group. Default value: -1 Maximum value: 31536000

relExpiryMilliSec Relative expiry time, in milliseconds, after which to expire an object cached in this content group. Default value: -1 Maximum value: 86400000

absExpiry Local time, up to 4 times a day, at which all objects in the content group must expire.

CLI Users: For example, to specify that the objects in the content group should expire by 11:00 PM, type the following command: add cache contentgroup <contentgroup name> -absexpiry 23:00 To specify that the objects in the content group should expire at 10:00 AM, 3 PM, 6 PM, and 11:00 PM, type: add cache contentgroup <contentgroup name> -absexpiry 10:00 15:00 18:00 23:00

absExpiryGMT Coordinated Universal Time (GMT), up to 4 times a day, when all objects in the content group must expire.

weakNegRelExpiry Relative expiry time, in seconds, for expiring negative responses. This value is used only if the expiry time cannot be determined from any other source. It is applicable only to the following status codes: 307, 403, 404, and 410. Default value: -1 Maximum value: 31536000

hitParams Parameters to use for parameterized hit evaluation of an object. Up to 128 parameters can be specified. Mutually exclusive with the Hit Selector parameter.

invalParams Parameters for parameterized invalidation of an object. You can specify up to 8 parameters. Mutually exclusive with invalSelector.

ignoreParamValueCase Ignore case when comparing parameter values during parameterized hit evaluation. (Parameter value case is ignored by default during parameterized invalidation.)

Possible values: YES, NO Default value: VAL_NOT_SET

matchCookies Evaluate for parameters in the cookie header also.

Possible values: YES, NO Default value: VAL_NOT_SET

invalRestrictedToHost Take the host header into account during parameterized invalidation.

Possible values: YES, NO Default value: VAL_NOT_SET

pollEveryTime Always poll for the objects in this content group. That is, retrieve the objects from the origin server whenever they are requested.

Possible values: YES, NO Default value: NO

ignoreReloadReq Ignore any request to reload a cached object from the origin server. To guard against Denial of Service attacks, set this parameter to YES. For RFC-compliant behavior, set it to NO.

Possible values: YES, NO Default value: YES

removeCookies Remove cookies from responses.

Possible values: YES, NO Default value: YES

prefetch Attempt to refresh objects that are about to go stale.

Possible values: YES, NO Default value: YES

prefetchPeriod Time period, in seconds before an object's calculated expiry time, during which to attempt prefetch. Default value: -1 Maximum value: 4294967294

prefetchPeriodMilliSec Time period, in milliseconds before an object's calculated expiry time, during which to attempt prefetch. Default value: -1 Maximum value: 4294967290

prefetchMaxPending Maximum number of outstanding prefetches that can be queued for the content group. Default value: -1 Minimum value: 0 Maximum value: 4294967294

flashCache Perform flash cache. Mutually exclusive with Poll Every Time (PET) on the same content group.

Possible values: YES, NO Default value: NO

expireAtLastByte Force expiration of the content immediately after the response is downloaded (upon receipt of the last byte of the response body). Applicable only to positive responses.

Possible values: YES, NO Default value: NO

insertVia Insert a Via header into the response.

Possible values: YES, NO Default value: YES

insertAge Insert an Age header into the response. An Age header contains information about the age of the object, in seconds, as calculated by the integrated cache.

Possible values: YES, NO Default value: YES

insertETag Insert an ETag header in the response. With ETag header insertion, the integrated cache does not serve full responses on repeat requests.

Possible values: YES, NO Default value: YES

cacheControl Insert a Cache-Control header into the response.

quickAbortSize If the size of an object that is being downloaded is less than or equal to the quick abort value, and a client aborts during the download, the cache stops downloading the response. If the object is larger than the quick abort size, the cache continues to download the response. Default value: 4194303 Maximum value: 4194303

minResSize Minimum size of a response that can be cached in this content group. Default minimum response size is 0. Maximum value: 2097151

maxResSize Maximum size of a response that can be cached in this content group. Default value: 80 Maximum value: 2097151

memLimit Maximum amount of memory that the cache can use. The effective limit is based on the available memory of the Citrix ADC. Default value: 65536

ignoreReqCachingHdrs Ignore Cache-Control and Pragma headers in the incoming request.

Possible values: YES, NO Default value: YES

minHits Number of hits that qualifies a response for storage in this content group. Default value: 0

alwaysEvalPolicies Force policy evaluation for each response arriving from the origin server. Cannot be set to YES if the Prefetch parameter is also set to YES.

Possible values: YES, NO Default value: NO

persistHA Setting persistHA to YES causes IC to save objects in contentgroup to Secondary node in HA deployment.

Possible values: YES, NO Default value: NO

pinned Do not flush objects from this content group under memory pressure.

Possible values: YES, NO Default value: NO

lazyDnsResolve Perform DNS resolution for responses only if the destination IP address in the request does not match the destination IP address of the cached response.

Possible values: YES, NO Default value: YES

hitSelector Selector for evaluating whether an object gets stored in a particular content group. A selector is an abstraction for a collection of PIXL expressions.

invalSelector Selector for invalidating objects in the content group. A selector is an abstraction for a collection of PIXL expressions.

type The type of the content group.

Possible values: HTTP, MYSQL, MSSQL Default value: HTTP

rm cache contentGroup

Removes the specified content group. Before removing, make sure that no cache policy has its storeInGroup attribute set to this group, otherwise the group cannot be removed.

Synopsis

rm cache contentGroup <name>

Arguments

name Name of the content group to be removed.

save cache contentGroup

Save the objects in the specified content group.

Synopsis

save cache contentGroup <name>

Arguments

name The name of the content group whose objects are to be save.

tosecondary content group whose objects are to be sent to secondary.

Possible values: YES, NO Default value: NO

flush cache contentGroup

Flush the objects in the specified content group.

Synopsis

flush cache contentGroup <name>

Arguments

name Name of the content group from which to flush objects, or "all" to flush all content groups.

query Query string specifying individual objects to flush from this group by using parameterized invalidation. If this parameter is not set, all objects are flushed from the group.

host Flush only objects that belong to the specified host. Do not use except with parameterized invalidation. Also, the Invalidation Restricted to Host parameter for the group must be set to YES.

selectorValue Value of the selector to be used for flushing objects from the content group. Requires that an invalidation selector be configured for the content group.

set cache contentGroup

Modifies the specified attributes of the content group.

Synopsis

set cache contentGroup <name>

Arguments

name Name of the content group to be modified.

weakPosRelExpiry Relative expiry time, in seconds, for expiring positive responses with response codes between 200 and 399. Cannot be used in combination with other Expiry attributes. Similar to -relExpiry but has lower precedence. Maximum value: 31536000

heurExpiryParam Heuristic expiry time, in percent of the duration, since the object was last modified. Minimum value: 0 Maximum value: 100

relExpiry Relative expiry time, in seconds, after which to expire an object cached in this content group. Default value: -1 Maximum value: 31536000

relExpiryMilliSec Relative expiry time, in milliseconds, after which to expire an object cached in this content group. Default value: -1 Maximum value: 86400000

absExpiry Local time, up to 4 times a day, at which all objects in the content group must expire.

CLI Users: For example, to specify that the objects in the content group should expire by 11:00 PM, type the following command: add cache contentgroup <contentgroup name> -absexpiry 23:00 To specify that the objects in the content group should expire at 10:00 AM, 3 PM, 6 PM, and 11:00 PM, type: add cache contentgroup <contentgroup name> -absexpiry 10:00 15:00 18:00 23:00

absExpiryGMT Coordinated Universal Time (GMT), up to 4 times a day, when all objects in the content group must expire.

weakNegRelExpiry Relative expiry time, in seconds, for expiring negative responses. This value is used only if the expiry time cannot be determined from any other source. It is applicable only to the following status codes: 307, 403, 404, and 410. Maximum value: 31536000

hitParams Parameters to use for parameterized hit evaluation of an object. Up to 128 parameters can be specified. Mutually exclusive with the Hit Selector parameter.

invalParams Parameters for parameterized invalidation of an object. You can specify up to 8 parameters. Mutually exclusive with invalSelector.

ignoreParamValueCase Ignore case when comparing parameter values during parameterized hit evaluation. (Parameter value case is ignored by default during parameterized invalidation.)

Possible values: YES, NO

matchCookies Evaluate for parameters in the cookie header also.

Possible values: YES, NO

invalRestrictedToHost Take the host header into account during parameterized invalidation.

Possible values: YES, NO

pollEveryTime Always poll for the objects in this content group. That is, retrieve the objects from the origin server whenever they are requested.

Possible values: YES, NO Default value: NO

ignoreReloadReq Ignore any request to reload a cached object from the origin server. To guard against Denial of Service attacks, set this parameter to YES. For RFC-compliant behavior, set it to NO.

Possible values: YES, NO Default value: YES

removeCookies Remove cookies from responses.

Possible values: YES, NO Default value: YES

prefetch Attempt to refresh objects that are about to go stale.

Possible values: YES, NO Default value: YES

prefetchPeriod Time period, in seconds before an object's calculated expiry time, during which to attempt prefetch. Default value: -1 Maximum value: 4294967294

prefetchPeriodMilliSec Time period, in milliseconds before an object's calculated expiry time, during which to attempt prefetch. Default value: -1 Maximum value: 4294967290

prefetchMaxPending Maximum number of outstanding prefetches that can be queued for the content group. Minimum value: 0 Maximum value: 4294967294

flashCache Perform flash cache. Mutually exclusive with Poll Every Time (PET) on the same content group.

Possible values: YES, NO Default value: NO

expireAtLastByte Force expiration of the content immediately after the response is downloaded (upon receipt of the last byte of the response body). Applicable only to positive responses.

Possible values: YES, NO Default value: NO

insertVia Insert a Via header into the response.

Possible values: YES, NO Default value: YES

insertAge Insert an Age header into the response. An Age header contains information about the age of the object, in seconds, as calculated by the integrated cache.

Possible values: YES, NO Default value: YES

insertETag Insert an ETag header in the response. With ETag header insertion, the integrated cache does not serve full responses on repeat requests.

Possible values: YES, NO Default value: YES

cacheControl Insert a Cache-Control header into the response.

quickAbortSize If the size of an object that is being downloaded is less than or equal to the quick abort value, and a client aborts during the download, the cache stops downloading the response. If the object is larger than the quick abort size, the cache continues to download the response. Maximum value: 4194303

minResSize Minimum size of a response that can be cached in this content group. Default minimum response size is 0. Maximum value: 2097151

maxResSize Maximum size of a response that can be cached in this content group. Default value: 80 Maximum value: 2097151

memLimit Maximum amount of memory that the cache can use. The effective limit is based on the available memory of the Citrix ADC. Default value: 65536

ignoreReqCachingHdrs Ignore Cache-Control and Pragma headers in the incoming request.

Possible values: YES, NO Default value: YES

minHits Number of hits that qualifies a response for storage in this content group.

alwaysEvalPolicies Force policy evaluation for each response arriving from the origin server. Cannot be set to YES if the Prefetch parameter is also set to YES.

Possible values: YES, NO Default value: NO

persistHA The option for IC objects to save objects to Secondary in a HA deployment. Set YES for IC to take this state.

Possible values: YES, NO Default value: NO

pinned The option for IC from flushing objects from this contentgroup under memory pressure. Set YES for IC to take this state.

Possible values: YES, NO Default value: NO

lazyDnsResolve Perform DNS resolution for responses only if the destination IP address in the request does not match the destination IP address of the cached response.

Possible values: YES, NO Default value: YES

hitSelector Selector for evaluating whether an object gets stored in a particular content group. A selector is an abstraction for a collection of PIXL expressions.

invalSelector Selector for invalidating objects in the content group. A selector is an abstraction for a collection of PIXL expressions.

stat cache contentGroup

Displays a summary of cache group statistics.

Synopsis

stat cache contentGroup

Arguments

name Name of the cache contentgroup for which to display statistics. If you do not set this parameter, statistics are shown for all cache contentgroups.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

non304 Hits for Content group (non304hit) Non304 hits for ContentGroup

304 Hits for Content group (304hit) 304 hits for ContentGroup

Number of objects in contentgroup (cell) Number of objects in contentgroup

Number of marker objects in contentgroup (Mrkcell) Number of marker objects in contentgroup

Number of times contentgroup is flushed (flushed) Number of times contentgroup is flushed

current memory usage (CurMem) current memory usage

maximum memory usage limit (MaxMem) maximum memory usage limit

Example

stat cache contentgroup

Related Commands

- stat cache policylabel

expire cache contentGroup

Forces expiration of all the objects in the specified content group. The next request for any object in the group is sent to the origin server.

Synopsis

expire cache contentGroup <name>

Arguments

name Name of the content group whose objects are to be expired.

show cache contentGroup

Displays information about all content groups, or about the specified content group.

Synopsis

show cache contentGroup

Arguments

name Name of the content group about which to display information.

Output

flags Flags.

type The type of the content group.

relExpiry The relative expiry time in seconds.

relExpiryMilliSec Relative expiry time, in milliseconds, after which to expire an object cached in this content group.

absExpiry Local time, up to 4 times a day, at which all objects in the content group must expire.

CLI Users: For example, to specify that the objects in the content group should expire by 11:00 PM, type the following command: add cache contentgroup <contentgroup name> -absexpiry 23:00 To specify that the objects in the content group should expire at 10:00 AM, 3 PM, 6 PM, and 11:00 PM, type: add cache contentgroup <contentgroup name> -absexpiry 10:00 15:00 18:00 23:00

absExpiryGMT Coordinated Universal Time (GMT), up to 4 times a day, when all objects in the content group must expire.

heurExpiryParam Heuristic expiry time, in percent of the duration, since the object was last modified.

weakPosRelExpiry Relative expiry time, in seconds, for expiring positive responses with response codes between 200 and 399. Cannot be used in combination with other Expiry attributes. Similar to -relExpiry but has lower precedence.

weakNegRelExpiry Relative expiry time, in seconds, for expiring negative responses. This value is used only if the expiry time cannot be determined from any other source. It is applicable only to the following status codes: 307, 403, 404, and 410.

hitParams Parameters to use for parameterized hit evaluation of an object. Up to 128 parameters can be specified. Mutually exclusive with the Hit Selector parameter.

invalParams Parameters for parameterized invalidation of an object. You can specify up to 8 parameters. Mutually exclusive with invalSelector.

ignoreParamValueCase Ignore case when comparing parameter values during parameterized hit evaluation. (Parameter value case is ignored by default during parameterized invalidation.)

matchCookies Evaluate for parameters in the cookie header also.

invalRestrictedToHost Take the host header into account during parameterized invalidation.

pollEveryTime Always poll for the objects in this content group. That is, retrieve the objects from the origin server whenever they are requested.

ignoreReloadReq Ignore any request to reload a cached object from the origin server. To guard against Denial of Service attacks, set this parameter to YES. For RFC-compliant behavior, set it to NO.

removeCookies Remove cookies from responses.

prefetch Attempt to refresh objects that are about to go stale.

prefetchPeriod Time period, in seconds before an object's calculated expiry time, during which to attempt prefetch.

prefetchPeriodMilliSec Time period, in milliseconds before an object's calculated expiry time, during which to attempt prefetch.

prefetchCur Current outstanding prefetches.

prefetchMaxPending Maximum number of outstanding prefetches that can be queued for the content group.

flashCache Perform flash cache. Mutually exclusive with Poll Every Time (PET) on the same content group.

expireAtLastByte Force expiration of the content immediately after the response is downloaded (upon receipt of the last byte of the response body). Applicable only to positive responses.

insertVia Insert a Via header into the response.

insertAge Insert an Age header into the response. An Age header contains information about the age of the object, in seconds, as calculated by the integrated cache.

insertETag Insert an ETag header in the response. With ETag header insertion, the integrated cache does not serve full responses on repeat requests.

cacheControl Insert a Cache-Control header into the response.

quickAbortSize If the size of an object that is being downloaded is less than or equal to the quick abort value, and a client aborts during the download, the cache stops downloading the response. If the object is larger than the quick abort size, the cache continues to download the response.

minResSize Minimum size of a response that can be cached in this content group. Default minimum response size is 0.

maxResSize Maximum size of a response that can be cached in this content group.

memUsage Current memory usage.

memDUsage Current disk memory usage.

diskLimit Maximum amount of disk that the cache can use. The effective limit is based on the available memory of the Citrix ADC.

memLimit Maximum amount of memory that the cache can use. The effective limit is based on the available memory of the Citrix ADC.

ignoreReqCachingHdrs Ignore Cache-Control and Pragma headers in the incoming request.

cacheNon304Hits Cache non 304 hits.

cache304Hits Cache 304 hits.

cacheCells Number of cells.

cacheGroupIncarnation Cache group incarnation.

minHits Number of hits that qualifies a response for storage in this content group.

alwaysEvalPolicies Force policy evaluation for each response arriving from the origin server. Cannot be set to YES if the Prefetch parameter is also set to YES.

persist Setting persist to YES causes IC to save objects in contentgroup to disk.

persistHA Setting persistHA to YES causes IC to save objects in contentgroup to Secondary node in HA deployment.

pinned Do not flush objects from this content group under memory pressure.

lazyDnsResolve Perform DNS resolution for responses only if the destination IP address in the request does not match the destination IP address of the cached response.

hitSelector Selector for evaluating whether an object gets stored in a particular content group. A selector is an abstraction for a collection of PIXL expressions.

invalSelector Selector for invalidating objects in the content group. A selector is an abstraction for a collection of PIXL expressions.

policyName Active cache policies refering to this group.

cacheNumInvalPolicy Number of active Invalidation policies refering to this group.

markerCells Numbers of marker cells in this group.

builtin feature The feature to be checked while applying this config

devno count stateflag

unset cache contentGroup

Use this command to remove cache contentGroup settings.Refer to the set cache contentGroup command for meanings of the arguments.

Synopsis

unset cache contentGroup <name>

cache-forwardProxy

The following operations can be performed on "cache-forwardProxy":

add| show| rm|

add cache forwardProxy

Allows the cache to act as a forward proxy for other Citrix ADCs or cache servers.

Synopsis

add cache forwardProxy <IPAddress> <port>

Arguments

IPAddress IP address of the Citrix ADC or a cache server for which the cache acts as a proxy. Requests coming to the Citrix ADC with the configured IP address are forwarded to the particular address, without involving the Integrated Cache in any way.

port Port on the Citrix ADC or a server for which the cache acts as a proxy Minimum value: 1

show cache forwardProxy

Displays the IP address and the corresponding ports for which the cache acted as a forward proxy.

Synopsis

show cache forwardProxy

Arguments

Output

IPAddress IP address of the Citrix ADC or a cache server for which the cache acts as a proxy. Requests coming to the Citrix ADC with the configured IP address are forwarded to the particular address, without involving the Integrated Cache in any way.

port Forward proxy port.

devno count stateflag

rm cache forwardProxy

Removes the forward proxy address from the Integrated Cache. The cache does not act as a proxy to the specified IP address.

Synopsis

rm cache forwardProxy <IPAddress> <port>

Arguments

IPAddress IP address of the Citrix ADC or a server for which the cache was as a proxy.

port Port on the Citrix ADC or a server for which the cache acts as a proxy Minimum value: 1

cache-global

The following operations can be performed on "cache-global":

show| unbind| bind|

show cache global

Displays the global bindings for cache policies.

Synopsis

show cache global

Arguments

type The bind point to which policy is bound. When you specify the type, detailed information about that bind point appears.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, HTTPQUIC_RES_OVERRIDE, HTTPQUIC_RES_DEFAULT

Output

policyName Name of the cache policy.

policy Name of the cache policy.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke Invoke policies bound to a virtual server or a user-defined policy label. After the invoked policies are evaluated, the flow returns to the policy with the next priority. Applicable only to default-syntax policies.

labelType Type of policy label to invoke.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE. (To invoke a label associated with a virtual server, specify the name of the virtual server.)

numpol The number of policies bound to the bindpoint.

flowType flowtype of the bound cache policy.

rule The request/response rule that will trigger the given action.

action The integrated cache action to be applied when the system sees content that matches the rules.

storeInGroup The content group to store the object when the action directive is CACHE.

invalGroups The content group(s) to be invalidated when the action directive is INVAL.

invalObjects The content group(s) whose objects will be invalidated when the action directive is INVAL.

hits Hits.

flags Flags.

precedeDefRules Override the default request/response cacheability rules.

stateflag globalBindType devno count

Example

show cache global

unbind cache global

Deactivate the policy by unbinding it from a global bind point.

Synopsis

unbind cache global <policy>

Arguments

policy Name of the policy to unbind.

type Bind point from which to unbind the policy.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, HTTPQUIC_RES_OVERRIDE, HTTPQUIC_RES_DEFAULT

priority Priority of the NOPOLICY to be unbound. Required only you want to unbind a NOPOLICY that might have been bound to this policy label. Minimum value: 1 Maximum value: 2147483647

bind cache global

Binds the cache policy to one of the two global bind points (an unnamed policy label invoked at request time and an unnamed policy label invoked at the response time). The flow type of the policy implicitly determines which label it gets bound to. A policy becomes active only when it is bound. A globally bound policy, it is available to all virtual servers on the Citrix ADC. All HTTP traffic is evaluated against the global policy labels. Each label contains an ordered list ordered by policies' priority values.

Synopsis

bind cache global <policy> -priority <positive_integer>

Arguments

policy Name of the policy to bind. (A policy must be created before it can be bound.)

priority Priority to assign to the policy. The appliance might disallow some priority values, depending on what you have already configured. For example, a response cache policy cannot have a higher priority than a request cache policy. Priority helps in dictating the order of policy evaluation. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the priority of the next policy to evaluate if the current policy rule evaluates to TRUE. Specify one of the following values:

- END. Terminate evaluation of this policy bank. This setting is equivalent to omitting the parameter.
- NEXT. Evaluate the policy with the next higher priority.
- An expression whose evaluation results in a number. Evaluation of an expression determines the next action as follows:
- If the expression evaluates to a priority number larger than the highest priority number in the policy bank, the next policy bank is evaluated.
- If the expression evaluates to the priority of a policy with a lower priority (higher number) within the same policy bank, that policy is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next-lower priority is evaluated next. Any of the following results trigger an UNDEF condition
- The expression cannot be evaluated.
- The expression evaluates to a number that is smaller than the current policy's priority number

type Bind point to which to bind the policy. Available settings function as follows:

- REQ_OVERRIDE. Binds the policy to the override request queue.
- REQ_DEFAULT. Binds the policy to the default request queue.
- RES_OVERRIDE. Binds the policy to the override response queue.
- RES_DEFAULT. Binds the policy to the default response queue.
- HTTPQUIC_REQ_OVERRIDE - Binds the policy to the HTTP_QUIC override request queue.
- HTTPQUIC_REQ_DEFAULT - Binds the policy to the HTTP_QUIC default request queue.
- HTTPQUIC_RES_OVERRIDE - Binds the policy to the HTTP_QUIC override response queue.
- HTTPQUIC_RES_DEFAULT - Binds the policy to the HTTP_QUIC default response queue.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, HTTPQUIC_RES_OVERRIDE, HTTPQUIC_RES_DEFAULT

invoke Invoke policies bound to a virtual server or a user-defined policy label. After the invoked policies are evaluated, the flow returns to the policy with the next priority. Applicable only to default-syntax policies.

labelType Type of policy label to invoke.

Possible values: reqvserver, resvserver, policylabel

labelName Name of the label to invoke if the current policy rule evaluates to TRUE. (To invoke a label associated with a virtual server, specify the name of the virtual server.)

cache-object

The following operations can be performed on "cache-object":

save| show| expire| flush|

save cache object

Save a cached object to local disk.

Synopsis

save cache object

Arguments

locator The ID of the cached object. Minimum value: 0

tosecondary Object will be saved onto Secondary.

Possible values: YES, NO Default value: NO

show cache object

Displays a list of all cached objects. The list displays the unique locator ID of each cached object along with the content group in which it was cached, and other details. To view more details of a specific cached object, use the -locator parameter along with this command.

Synopsis

show cache object [(-url <URL> (-host <string>)) | -locator <positive_integer> | -httpStatus <positive_integer> | -group <string> | -ignoreMarkerObjects (ON | OFF) | -includeNotReadyObjects (ON | OFF)]

Arguments

url URL of the particular object whose details is required. Parameter "host" must be specified along with the URL.

locator ID of the cached object. Minimum value: 0

httpStatus HTTP status of the object. Minimum value: 0

host Host name of the object. Parameter "url" must be specified.

port Host port of the object. You must also set the Host parameter. Default value: 80 Minimum value: 1

groupName Name of the content group to which the object belongs. It will display only the objects belonging to the specified content group. You must also set the Host parameter.

httpMethod HTTP request method that caused the object to be stored.

Possible values: GET, POST Default value: GET

group Name of the content group whose objects should be listed.

ignoreMarkerObjects Ignore marker objects. Marker objects are created when a response exceeds the maximum or minimum response size for the content group or has not yet received the minimum number of hits for the content group.

Possible values: ON, OFF

includeNotReadyObjects Include responses that have not yet reached a minimum number of hits before being cached.

Possible values: ON, OFF

Output

cacheResSize Cache response size of the object.

cacheResHdrSize Cache response header size of the object.

cacheETag Cache ETag of the object.

httpStatusOutput HTTP status of the object.

cacheResLastMod Value of "Last-modified" header.

cacheControl Cache-Control header of the object.

cacheResDate Value of "Date" header

contentGroup Name of the contentgroup in which it is stored.

destIP Destination IP.

destIPV46 Destination IP.

destPort Destination Port.

cacheCellComplex The state of the parameterized caching on this cell.

hitParams Parameterized hit evaluation of an object.

hitValues Values of hitparams for this object.

cacheCellReqTime Required time of the cache cell object.

cacheCellResTime Response time to the cache cell object.

cacheCurAge Current age of the cache object.

cacheCellExpires Expiry time of the cache cell object in seconds.

cacheCellExpiresMilliSec Expiry time of the cache cell object in milliseconds.

flushed Specifies whether the object is flushed.

prefetch Specifies whether Integrated Cache should attempt to refresh an object immediately before it goes stale.

prefetchPeriod The duration in seconds of the period during which prefetch should be attempted, immediately before the object's calculated expiry time.

prefetchPeriodMilliSec The duration in milliseconds of the period during which prefetch should be attempted, immediately before the object's calculated expiry time.

cacheCellCurReaders Current readers of the cache cell object.

cacheCellCurMisses Current misses of the cache cell object.

cacheCellHits Cache cell hits.

cacheCellMisses Cache cell misses.

cacheCellDHits Cache cell disk hits.

cacheCellGzipCompressed The state of the response being gzip-compressed.

cacheCellDeflateCompressed The state of the response being deflate-compressed.

cacheCellCompressionFormat Compression format of this object. Identity means not compressed

cacheCellAppFWMetadataExists AppFirewall cache object.

cacheCellHttp11 The state of the response to be HTTP/1.1.

cacheCellWeakEtag The state of the weak HTTP Entity Tag in the cell.

cacheCellResBadSize The marked state of the cell.

markerReason Reason for marking the cell.

cacheCellPollEveryTime The state to poll every time on object.

cacheCellEtagInserted The state of the ETag to be inserted by IC for this object.

cacheCellReadyWithLastByte The state of the complete arrived response.

cacheInMemory The cache data is available in memory.

cacheInDisk The cache data is available in disk.

cacheInSecondary The cache data is available in secondary in HA deployment.

cacheDirname The directory name used if saved.

cacheFilename The filename used if saved.

cacheCellDestipVerified The state of DNS verification.

cacheCellFwpxyObj The state of the object to be stored on a request to a forward proxy.

cacheCellBasefile The state of delta being used as a basefile.

cacheCellMinHitFlag The state of the minhit feature on this cell.

cacheCellMinHit Min hit value for the object.

policy Policy info for the object.

policyName Policy which created the object.

selectorName The hit selector for the object.

rule Selectors for this object.

selectorValue The HTTP request method that caused the object to be stored.

cacheUrls List of cache object URLs.

numurls Total number of cache object entries returned in cacheUrls field

warnBucketSkip Bucket skipped warning.

totalObjs Total objects.

httpCalloutCell Is it a http callout cell ?

httpCalloutName Name of the http callout

returnType Return type of the http callout

httpCalloutResult First few bytes of http callout response

locatorshow ID of the cached object.

ceflags Indicates state and type of cached cell

devno count stateflag

expire cache object

Forces expiry of a cached object. You have to specify the locator ID of the cached object by using the -locator parameter.

Synopsis

expire cache object (-locator <positive_integer> | (-url <URL> (-host <string>)))

Arguments

locator ID of the cached object to be expired To view the locator ID of the cached objects, use the show cache object command. Minimum value: 0

url The URL of the object to be expired.

host The host of the object to be expired.

port The host port of the object to be expired. Default value: 80 Minimum value: 1

groupName Name of the content group to which the object belongs.

httpMethod HTTP request method that caused the object to be stored.

Possible values: GET, POST Default value: GET

flush cache object

Removes a cached object from memory and from disk (if it has a disk copy). You have to specify the locator ID of the cached object by using the -locator parameter

Synopsis

flush cache object (-locator <positive_integer> | (-url <URL> (-host <string>)))

Arguments

locator ID of the cached object. To view the locator ID of the cached objects, use the show cache object command. Minimum value: 0

url URL of the object to be flushed. You must also set the Host parameter.

host Host of the object to be flushed. Must provide the "url" parameter along with the host.

port Host port of the object to be flushed. Must provide the "host" parameter along with the port. Default value: 80 Minimum value: 1

groupName Name of the content group to which the object belongs. Must provide the \"host\" parameter along with the group name.

httpMethod HTTP request method that caused the object to be stored. All objects cached by that method will be flushed.

Possible values: GET, POST Default value: GET

cache-parameter

The following operations can be performed on "cache-parameter":

show| set| unset|

show cache parameter

Displays the global configuration of the Integrated Cache.

Synopsis

show cache parameter

Arguments

Output

diskLimit The disk limit for the Integrated Cache.

maxDiskLimit The maximum value of the memory limit for the Integrated Cache.

memLimit The memory limit for the Integrated Cache.

memLimitActive Active value of the memory limit for the Integrated Cache.

maxMemLimit The maximum value of the memory limit for the Integrated Cache.

via The string that is inserted in the "Via" header.

verifyUsing The criteria for deciding whether a cached object can be served for an incoming HTTP request.

maxPostLen The maximum POST body size that the IC can accumulate.

prefetchCur Number of current outstanding prefetches in the IC.

prefetchMaxPending The maximum number of outstanding prefetches on the content group.

enableBypass When this value is set to NO, an incoming request will serve a hit if a matching object is found in cache storage, regardless of the cacheability policy configuration. If set to YES, the bound request cacheability policies are evaluated before attempting any hit selection in the cache storage. If the request matches a policy with a NOCACHE action, the request will bypass all cache processing. This flag does not affect processing of requests that match any invalidation policy.

undefAction Action to take when a policy cannot be evaluated.

enableHaObjPersist The HA object persisting parameter. When this value is set to YES, cache objects can be synced to Secondary in a HA deployment. If set to NO, objects will never be syned to Secondary node.

set cache parameter

Modifies the global configuration of the integrated cache. You can modify the settings of various parameters.

Synopsis

set cache parameter

Arguments

memLimit Amount of memory available for storing the cache objects. In practice, the amount of memory available for caching can be less than half the total memory of the Citrix ADC.

via String to include in the Via header. A Via header is inserted into all responses served from a content group if its Insert Via flag is set.

verifyUsing Criteria for deciding whether a cached object can be served for an incoming HTTP request. Available settings function as follows: HOSTNAME - The URL, host name, and host port values in the incoming HTTP request header must match the cache policy. The IP address and the TCP port of the destination host are not evaluated. Do not use the HOSTNAME setting unless you are certain that no rogue client can access a rogue server through the cache. HOSTNAME_AND_IP - The URL, host name, host port in the incoming HTTP request header, and the IP address and TCP port of the destination server, must match the cache policy. DNS - The URL, host name and host port in the incoming HTTP request, and the TCP port must match the cache policy. The host name is used for DNS lookup of the destination server's IP address, and is compared with the set of addresses returned by the DNS lookup.

Possible values: HOSTNAME, HOSTNAME_AND_IP, DNS

maxPostLen Maximum number of POST body bytes to consider when evaluating parameters for a content group for which you have configured hit parameters and invalidation parameters. Default value: 4096 Minimum value: 0 Maximum value: 131072

prefetchMaxPending Maximum number of outstanding prefetches in the Integrated Cache. Minimum value: 0

enableBypass Evaluate the request-time policies before attempting hit selection. If set to NO, an incoming request for which a matching object is found in cache storage results in a response regardless of the policy configuration. If the request matches a policy with a NOCACHE action, the request bypasses all cache processing. This parameter does not affect processing of requests that match any invalidation policy.

Possible values: YES, NO

undefAction Action to take when a policy cannot be evaluated.

Possible values: NOCACHE, RESET

enableHaObjPersist The HA object persisting parameter. When this value is set to YES, cache objects can be synced to Secondary in a HA deployment. If set to NO, objects will never be synced to Secondary node.

Possible values: YES, NO Default value: NO

unset cache parameter

Use this command to remove cache parameter settings.Refer to the set cache parameter command for meanings of the arguments.

Synopsis

unset cache parameter

cache-policy

The following operations can be performed on "cache-policy":

rename| add| rm| set| unset| show| stat|

rename cache policy

Renames an existing cache policy.

Synopsis

rename cache policy <policyName>@ <newName>@

Arguments

policyName Existing name of the cache policy.

newName New name for the cache policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

Example

rename cache policy oldname newname

add cache policy

Creates an integrated caching policy. The newly created policy is in inactive state. To activate the policy, use the bind cache global command.

Synopsis

add cache policy <policyName> -rule <expression> -action <action>

Arguments

policyName Name for the policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the policy is created.

rule Expression against which the traffic is evaluated. The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Action to apply to content that matches the policy.

- CACHE or MAY_CACHE action - positive cachability policy
- NOCACHE or MAY_NOCACHE action - negative cachability policy
- INVAL action - Dynamic Invalidation Policy

Possible values: CACHE, NOCACHE, MAY_CACHE, MAY_NOCACHE, INVAL

storeInGroup Name of the content group in which to store the object when the final result of policy evaluation is CACHE. The content group must exist before being mentioned here. Use the "show cache contentgroup" command to view the list of existing content groups.

invalGroups Content group(s) to be invalidated when the INVAL action is applied. Maximum number of content groups that can be specified is 16.

invalObjects Content groups(s) in which the objects will be invalidated if the action is INVAL.

undefAction Action to be performed when the result of rule evaluation is undefined.

Possible values: NOCACHE, RESET

rm cache policy

Removes the specified caching policy. Make sure that the policy is not bound globally or to a virtual server. A bound policy cannot be removed.

Synopsis

rm cache policy <policyName>

Arguments

policyName Name of the cache policy to be removed.

set cache policy

Modifies the specified attributes of an existing cache policy. The rule, flow type, can be changed only if action and undefAction (if present) are of NEUTRAL flow type.

Synopsis

set cache policy <policyName>

Arguments

policyName Name for the policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the policy is created.

rule Expression against which the traffic is evaluated. The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Action to apply to content that matches the policy.

- CACHE or MAY_CACHE action - positive cachability policy
- NOCACHE or MAY_NOCACHE action - negative cachability policy

- INVAL action - Dynamic Invalidation Policy

Possible values: CACHE, NOCACHE, MAY_CACHE, MAY_NOCACHE, INVAL

storeInGroup Name of the content group in which to store the object when the final result of policy evaluation is CACHE. The content group must exist before being mentioned here. Use the "show cache contentgroup" command to view the list of existing content groups.

invalGroups Content group(s) to be invalidated when the INVAL action is applied. Maximum number of content groups that can be specified is 16.

invalObjects Content groups(s) in which the objects will be invalidated if the action is INVAL.

undefAction Action to be performed when the result of rule evaluation is undefined.

Possible values: NOCACHE, RESET

Example

set cache policy pol9 -rule "http.req.HEADER(\\"header\\").CONTAINS(\\"qh2\\")"

unset cache policy

Use this command to remove cache policy settings.Refer to the set cache policy command for meanings of the arguments.

Synopsis

unset cache policy <policyName>

show cache policy

Displays all configured cache policies. To display details about a particular cache policy, specify the name of the policy. When all caching policies are displayed, the order of the displayed policies within each group is the same as the evaluation order of the policies. There are three groups: request policies, response policies, and dynamic invalidation policies.

Synopsis

show cache policy show cache policy stats - alias for 'stat cache policy'

Arguments

policyName Name of the cache policy about which to display details.

Output

stateflag rule The request/response rule that will trigger the specified action.

action The integrated cache action to be applied when the system sees content that matches the rules.

storeInGroup The content group that will store the object when the action directive is CACHE.

invalGroups The content group(s) to be invalidated when the action directive is INVAL.

invalObjects The content group(s) whose objects will be invalidated when the action directive is INVAL.

priority Priority.

hits Hits.

undefAction A CACHE action, to be used by the policy when the rule evaluation turns out to be undefined.

undefHits Number of Undef hits.

flags Flag.

precedeDefRules Override default request/response cacheability rules.

activePolicy Indicates whether policy is bound or not.

boundTo Location where policy is bound

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

bindPolicyType vserverType builtin feature The feature to be checked while applying this config

type devno count

stat cache policy

Displays a summary of cache policy statistics.

Synopsis

stat cache policy

Arguments

policyName Name of the cache policy for which to display statistics. If you do not set this parameter, statistics are shown for all cache policies.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Policy undef hits (Undefhits) Number of undef hits on the policy

Example

stat cache policy

Related Commands

- stat cache contentGroup

cache-policylabel

The following operations can be performed on "cache-policylabel":

rm| unbind| rename| show| add| stat| bind|

rm cache policylabel

Removes the specified integrated caching policy label.

Synopsis

rm cache policylabel <labelName>

Arguments

labelName Name of the label to be removed.

Example

rm cache policylabel cache_http_url

unbind cache policylabel

Unbinds a policy from a cache-policy label.

Synopsis

unbind cache policylabel <labelName> -policyName <string>

Arguments

labelName Name of the cache policy label from which to unbind the policy.

policyName Name of the policy to unbind from the label.

priority Required only if you want to unbind a NOPOLICY that might have been bound to this policy label. Minimum value: 1 Maximum value: 2147483647

Example

unbind cache policylabel cache_http_url pol_1

rename cache policylabel

Renames a cache-policy label.

Synopsis

rename cache policylabel <labelName>@ <newName>@

Arguments

labelName Existing name of the cache-policy label.

newName New name for the cache-policy label. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

Example

rename cache policylabel oldname newname

show cache policylabel

Displays information about all cache-policy labels or about the specified cache-policy label.

Synopsis

show cache policylabel

Arguments

labelName Name of the cache-policy label about which to display information.

Output

stateflag flags evaluates When to evaluate policies bound to this label: request-time or response-time.

numpol Number of polices bound to label.

hits Number of times policy label was invoked.

policyName Name of the cache policy to bind to the policy label.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke Invoke policies bound to a virtual server or a user-defined policy label. After the invoked policies are evaluated, the flow returns to the policy with the next-lower priority.

labelType Type of policy label to invoke: an unnamed label associated with a virtual server, or user-defined policy label.

labelName Name of the policy label to invoke if the current policy rule evaluates to TRUE.

flowType Flowtype of the bound cache policy.

builtin feature The feature to be checked while applying this config

devno count

Example

i)show cache policylabel cache_http_url ii)show cache policylabel

add cache policylabel

Creates a user-defined cache policy label. A policy label is a bind point of a group of policies.

Synopsis

add cache policylabel <labelName> -evaluates <evaluates>

Arguments

labelName Name for the label. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the label is created.

evaluates When to evaluate policies bound to this label: request-time or response-time.

Possible values: REQ, RES, MSSQL_REQ, MSSQL_RES, MYSQL_REQ, MYSQL_RES, HTTPQUIC_REQ, HTTPQUIC_RES

Example

add cache policylabel cache_http_url -evaluates REQ

stat cache policylabel

Displays statistics of cache policy label(s).

Synopsis

stat cache policylabel

Arguments

labelName Name of the cache-policy label for which to display statistics. If you do not set this parameter statistics are shown for all cache-policy labels.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy Label Hits (Hits) Number of times policy label was invoked.

Related Commands

- stat cache contentGroup

bind cache policylabel

Binds a cache policy to a policy label.

Synopsis

bind cache policylabel <labelName> -policyName <string> -priority <positive_integer>

Arguments

labelName Name of the cache policy label to which to bind the policy.

policyName Name of the cache policy to bind to the policy label.

priority Integer specifying the priority of this policy within the policy label. A lower number specifies a higher priority. The policies bound to the label are evaluated in the order of their priorities. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the priority of the next policy, within the policy label, to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher numbered priority.
- END - Stop evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, it's evaluation result determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, that policy is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher priority number is evaluated next.
- If the expression evaluates to a priority number that is numerically higher than the highest priority number, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

invoke Invoke policies bound to a virtual server or a user-defined policy label. After the invoked policies are evaluated, the flow returns to the policy with the next-lower priority.

labelType Type of policy label to invoke: an unnamed label associated with a virtual server, or user-defined policy label.

Possible values: reqvserver, resvserver, policylabel

labelName Name of the policy label to invoke if the current policy rule evaluates to TRUE.

Example

i)bind cache policylabel cache_http_url pol_1 1 2 -invoke reqvserver CURRENT ii)bind cache policylabel cache_http_url pol_2 2

cache-selector

The following operations can be performed on "cache-selector":

rm| add| show| set|

rm cache selector

Removes cache selectors. Note: A selector being used as a hit or invalidation selector in any content group cannot be removed without unsetting it from the content group.

Synopsis

rm cache selector <selectorName>

Arguments

selectorName Name of the selector.

add cache selector

Creates an Integrated Cache selector. A selector is an abstraction for a collection of PIXL expressions. After creating a selector, you can use it as a hit selector, invalidation selector, or both. You must specify at least one expression when you create a selector.

Synopsis

add cache selector <selectorName> <rule> ...

Arguments

selectorName Name for the selector. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

rule One or multiple PIXL expressions for evaluating an HTTP request or response.

show cache selector

Displays all cache selectors, or the specified.

Synopsis

show cache selector

Arguments

selectorName Name of the selector to display.

Output

flags Flags.

rule Rule.

builtin feature The feature to be checked while applying this config

devno count stateflag

set cache selector

Modify the set of PIXL expressions associated with a cache selector.

Synopsis

set cache selector <selectorName> <rule> ...

Arguments

selectorName Name of the selector to be modified.

rule One or multiple PIXL expressions for evaluating an HTTP request or response.

cache-stats

The following operations can be performed on "cache-stats":

show cache stats

show cache stats is an alias for stat cache

Synopsis

show cache stats - alias for 'stat cache'

cache

The following operations can be performed on "cache":

stat cache

Shows Integrated Cache performance statistics.

Synopsis

stat cache

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Maximum memory(KB) Deprecated (MaxMem) Largest amount of memory the Citrix ADC can dedicate to caching, up to 50% of available memory. A 0 value disables caching, but the caching module continues to run.

Recent successful reval ratio(%) (RPSucRev) Recently recorded percentage of times stored content was successfully revalidated by a 304 response rather than by a full response

Recent storable miss ratio(%) (RPctStMis) Recently recorded ratio of store-able misses to all misses expressed as percentage.

Recent parameterized 304 hit ratio(%) (RPPHit) Recently recorded ratio of parameterized 304 hits to all parameterized hits expressed as a percentage

Recent origin bandwidth saved(%) (RPOrBan) Bytes served from cache divided by total bytes served to client. This ratio can be greater than 1 because of the assumption that all compression has been done in the Citrix ADC.

Recent hit ratio(%) (RPctHit) Recently recorded cache hit ratio expressed as percentage

Recent byte hit ratio(%) (RPcByHit) Recently recorded cache byte hit ratio expressed as percentage. Here we define byte hit ratio as ((number of bytes served from the cache)/(total number of bytes served to the client)). This is the standard definition of Byte Hit Ratio. If compression is turned ON in NS then this ratio doesn't mean much. This might under or over estimate the origin-to-cache bandwidth saving (depending upon whether bytes served by CMP in Citrix ADC are more or less than compressed bytes served from the cache). If CMP is turned OFF in NS then this ratio is same as cacheRecentPercentOriginBandwidthSaved.

Recent 304 hit ratio(%) (RPct304Hit) Recently recorded ratio of 304 hits to all hits expressed as percentage

Utilized memory(KB) (UtiMem) Amount of memory the integrated cache is currently using.

Maximum memory active value(KB) (MaxMemActive) Currently active value of maximum memory

Maximum memory(KB) (Max64Mem) Largest amount of memory the Citrix ADC can dedicate to caching, up to 50% of available memory. A 0 value disables caching, but the caching module continues to run.

Poll every time hit ratio(%) (PPeHit) Percentage of cache hits in content groups that have Poll Every Time enabled, relative to all searches of content groups with Poll Every Time enabled.

Poll every time hits (PeHit) Number of times a cache hit was found during a search of a content group that has Poll Every Time enabled.

Parameterized 304 hit ratio(%) (PP304Hit) Percentage of parameterized 304 hits relative to all parameterized hits.

Total parameterized hits (PHit) Parameterized requests resulting in either a 304 or non-304 hit.

Successful reval ratio(%) (PSucRev) Percentage of times stored content was successfully revalidated by a 304 (Object Not Modifed) response rather than by a full response

Storable miss ratio(%) (PStrMiss) Responses that were fetched from the origin, stored in the cache, and then served to the client, as a percentage of all cache misses.

Conversions to conditional req (FuToCon) Number of user-agent requests for a cached Poll Every Time (PET) response that were sent to the origin server as conditional requests.

Successful revalidations (TSucRev) Total number of times stored content was successfully revalidated by a 304 Not Modified response from the origin.

Revalidations (Reval) Responses that an intervening cache revalidated with the integrated cache before serving, as determined by a Cache-Control: Max-Age header configurable in the integrated cache

Non-storable misses (NStrMiss) Cache misses for which the fetched response is not stored in the cache. These responses match policies with a NOCACHE action or are affected by Poll Every Time.

Storable misses (StrMiss) Cache misses for which the fetched response is stored in the cache before serving it to the client. Storable misses conform to a built-in or user-defined caching policy that contains a CACHE action.

Compressed bytes from cache (CmpBySer) Number of compressed bytes served from the cache

Byte hit ratio(%) (PByHit) Bytes served from the cache divided by total bytes served to the client. If compression is On in the Citrix ADC, this ratio may not reflect the bytes served by the compression module. If the compression is Off, this ratio is the same as cachePercentOriginBandwidthSaved.

Bytes served by cache (BySer) Total number of bytes served from the integrated cache

Bytes served by NetScaler (RespBy) Total number of HTTP response bytes served by Citrix ADC from both the origin and the cache

304 hit ratio(%) (Pct304Hit) 304 responses as a percentage of all responses that the Citrix ADC served.

Marker objects (NumMark) Marker objects created when a response exceeds the maximum or minimum size for entries in its content group or has not yet received the minimum number of hits required for items in its content group.

Origin bandwidth saved(%) (POrBan) Percentage of origin bandwidth saved, expressed as number of bytes served from the integrated cache divided by all bytes served. The assumption is that all compression is done in the Citrix ADC.

Hit ratio(%) (PctHit) Cache hits as percentage of the total number of requests

Misses (TotMiss) Intercepted HTTP requests requiring fetches from origin server.

Hits (TotHit) Responses served from the integrated cache. These responses match a policy with a CACHE action.

Requests (CacReq) Total cache hits plus total cache misses.

Cached objects (NumCac) Responses currently in integrated cache. Includes responses fully downloaded, in the process of being downloaded, and expired or flushed but not yet removed.

Hits being served (CacHit) This number should be close to the number of hits being served currently.

Misses being handled (CurMiss) Responses fetched from the origin and served from the cache. Should approximate storable misses. Does not include non-storable misses.

Non-304 hits (Non304Hit) Total number of full (non-304) responses served from the cache. A 304 status code indicates that a response has not been modified since the last time it was served

304 hits (304Hit) Object not modified responses served from the cache. (Status code 304 served instead of the full response.)

sql hits (sqlHit) sql response served from cache

Expire at last byte (ExpLa) Instances of content expiring immediately after receiving the last body byte due to the Expire at Last Byte setting for the content group.

Flashcache misses (FlMi) Number of requests to a content group with flash cache enabled that were cache misses. Flash cache distributes the response to all the clients in aqueue.

Flashcache hits (FlHi) Number of requests to a content group with flash cache enabled that were cache hits. The flash cache setting queues requests that arrive simultaneously and distributes the response to all the clients in the queue.

Parameterized inval requests (PInReq) Requests matching a policy with an invalidation (INVAL) action and a content group that uses an invalidation selector or parameters.

Full inval requests (NPInReq) Requests that match an invalidation policy where the invalGroups parameter is configured and expires one or more content groups.

Inval requests (INStrMis) Requests that match an invalidation policy and result in expiration of specific cached responses or entire content groups.

Parameterized requests (PReq) Total number of requests where the content group has hit and invalidation parameters or selectors.

Parameterized non-304 hits (PN304Hit) Parameterized requests resulting in a full response (not status code 304: Object Not Updated) served from the cache.

Parameterized 304 hits (P304Hit) Parameterized requests resulting in an object not modified (status code 304) response.

Poll every time requests (PeReq) Requests that triggered a search of a content group that has Poll Every Time (PET) enabled (always consult the origin server before serving cached data).

Memory allocation failures (ErrMem) Total number of times the cache failed to allocate memory to store responses.

Largest response so far(B) (LarResp) Size, in bytes, of largest response sent to client from the cache or the origin server.

Compressed bytes transmitted Number of bytes the Citrix ADC sends to the client after compressing the response from the server.

Compressible bytes received Number of bytes that can be compressed, which the Citrix ADC receives from the server. This gives the content length of the response that the Citrix ADC receives from server.

Response bytes received (HTRspbRx) Total number of bytes of HTTP response data received.

Related Commands

- stat cache contentGroup

cli

alias

The following operations can be performed on "alias":

alias

Create (short) aliases for (long) commands. Aliases are saved across NSCLI sessions. If no argument is specified, the alias command will display existing aliases.

Synopsis

alias [<pattern>]

Arguments

pattern Alias name. (Can be a regular expression.)

command Target command

Example

alias info "show ns info"

backup

The following operations can be performed on "backup":

backup

backup cache object to local disk

Synopsis

backup -pattern <string>

Arguments

pattern Name of the alias

Example

backup cache object -locator <id>

batch

The following operations can be performed on "batch":

batch

Use this command to read the contents of a file and execute each line as a separate CLI command. Each command in the file must be on a separate line. Lines starting with # are considered comments.

Synopsis

batch -fileName <input_filename>

Arguments

fileName The name of the batch file.

outfile The name of the file where the executed batch file will write its output. The default is standard output.

ntimes The number of times the batch file will be executed. Default value: 1 Minimum value: 0

Output

response

Example

batch -f cmds.txt

cli-attribute

The following operations can be performed on "cli-attribute":

show cli attribute

Display attributes of the Citrix ADC CLI

Synopsis

show cli attribute

Arguments

Output

qquote The construct that is used to quote strings that are to be taken as-is, without interpreting escape sequences like " ". This construct consists of: a 'q', followed by a delimiter character; the string follows immediately after the delimiter and is terminated by the first matching delimiter character. (The set of possible delimiter characters is listed below.) For example, q/a / will result in a three-character string ('a', '', 'n'); whereas "a " results in a two-character string ('a' followed by a newline).

qquoteDelimiters The set of characters that can be used as the delimiter in a q// construct. Characters shown in pairs must be used that way, whereas characters shown singly server as thier own matching delimiter. For example, q?abc? and q{abc} are valid q// constructs, and evaluate to the string "abc"; q{abc{ is however not a valid q// construct so it will evaluate to the string "q{abc{".

Cli

The entities on which you can perform NetScaler CLI operations:

- alias
- cli-attribute
- backup
- batch
- cls
- config
- exit
- help
- history
- man
- cli-mode
- cli-prompt
- quit
- source
- unalias

- whoami

cli-mode

The following operations can be performed on "cli-mode":

set| show| unset|

set cli mode

Use this command to specify how the CLI should display command output.

Synopsis

set cli mode

Arguments

page Determines whether output that spans more than one screen is "paged". Specify ON to pause the display after each screen of ouput.

Possible values: ON, OFF Default value: OFF

total Determines whether CLI "show" commands display a total count of objects before displaying the objects themselves.

Possible values: ON, OFF Default value: OFF

color Specifies whether output can be shown in color, if the terminal supports it.

Possible values: ON, OFF Default value: OFF

disabledFeatureAction Specifies what will happen when a configuration command is issued for a disabled feature. The following values are allowed: NONE - The action is allowed, and no warning message is issued.; ALLOW - The action is allowed, but a warning message is issued.; DENY - The action is not allowed.

Possible values: NONE, ALLOW, DENY Default value: NS_ALLOW

timeout CLI session inactivity timeout, in seconds. If Restrictedtimeout argument of system parameter is enabled, Timeout can have values in the range seconds and also climode timeout cannot be configured beyond admin configured value. If Restrictedtimeout argument of system parameter is disabled, Timeout can have values in the range seconds. Default value is 900 seconds. Default value: -1

regex If ON, regular expressions can be used as argument values

Possible values: ON, OFF Default value: ON

show cli mode

Use this command to display the current settings of parameters that can be set with the 'set cli mode' command.

Synopsis

show cli mode

Arguments

Output

page Determines whether output that spans more than one screen is "paged". Specify ON to pause the display after each screen of ouput.

total Determines whether CLI "show" commands display a total count of objects before displaying the objects themselves.

color Specifies whether output can be shown in color, if the terminal supports it.

disabledFeatureAction Specifies what will happen when a configuration command is issued for a disabled feature. The following values are allowed: NONE - The action is allowed, and no warning message is issued.; ALLOW - The action is allowed, but a warning message is issued.; DENY - The action is not allowed.

argMark mark

noLicenseAction no licence

diagLevel diagnostic level

timeout CLI session inactivity timeout, in seconds. If Restrictedtimeout argument of system parameter is enabled, Timeout can have values in the range seconds and also climode timeout cannot be configured beyond admin configured value. If Restrictedtimeout argument of system parameter is disabled, Timeout can have values in the range seconds. Default value is 900 seconds.

timeoutKind From where the timeout has been inherited.

regex If ON, regular expressions can be used as argument values

r regular expression

format format

stats serverPort

unset cli mode

Use this command to remove cli mode settings.Refer to the set cli mode command for meanings of the arguments.

Synopsis

unset cli mode

cli-prompt

The following operations can be performed on "cli-prompt":

set| show| clear|

set cli prompt

Use this command to customize the CLI prompt.

Synopsis

set cli prompt <promptString>

Arguments

promptString The prompt string. The following special values are allowed: %! - will be replaced by the history event number %u - will be replaced by the Citrix ADC user name %h - will be replaced by the Citrix ADC hostname %t - will be replaced by the current time %T - will be replaced by the current time (24 hr format) %d - will be replaced by the current date %s - will be replaced by the node state

Example

```
set cli prompt "%h %T" Done lb-ns1 15:16>
```

show cli prompt

Use this command to display the current CLI prompt, with special values like '%h' unexpanded.

Synopsis

show cli prompt

Arguments

Output

promptString

Example

10.101.4.22 15:20> sh cli prompt CLI prompt is set to "%h %T" Done

clear cli prompt

Use this command to return the CLI prompt to the default (a single '>').

Synopsis

clear cli prompt

cls

The following operations can be performed on "cls":

cls

Clear the screen and reposition cursor at top right.

Synopsis

cls

config

The following operations can be performed on "config":

config

Enter this command to enter contextual mode.

Synopsis

config

exit

The following operations can be performed on "exit":

exit

Use this command to back out one level in config mode, or to terminate the CLI when not in config mode.);

Synopsis

exit

help

The following operations can be performed on "help":

help

Use this command to display help information for a CLI command, for a group of commands, or for all CLI commands.

Synopsis

help

Arguments

commandName The name of a command for which you want full usage information.

groupName The name of a command group for which you want basic usage information.

all Use this option to request basic usage information for all commands.

Example

1.To view help information for adding a virtual server, enter the following CLI command: help add vserver The following information is displayed: Usage: add vserver <vServerName> <serviceType>

where: serviceType = (HTTP | FTP | TCP | UDP | SSL | SSL_BRIDGE | SSL_TCP | NNTP| DNS | ANY) <cacheType> = (TRANSPARENT | REVERSE | FORWARD) Done 2.To view help

information for all DNS commands, enter the following command: help dns The following information is displayed: add aaaaRec <hostname> <IPv6Address> ... rm aaaaRec <hostname> show aaaaRec add addRec <hostname> <IPAddress> ... rm addRec <hostname> show addRec add cnameRec <aliasName> <canonicalName> rm cnameRec <aliasName> show cnameRec add mxRec <domain> -mx <string> -pref <positive_integer> rm mxRec <domain> <mx> set mxRec <domain> -mx <string> show mxRec add nsRec <domain> rm nsRec <domain> show nsRec set dns parameter show dns parameter add soaRec <domain> -contact <string> -serial <positive_integer> -refresh <secs> -retry <secs> -expire <secs> -minimum <secs>-TTL <secs> rm soaRec <domain> set soaRec <domain> -serial <positive_integer> -minimum <secs> show soaRec add dns ptrRec <reverseDomain> <domain> ... rm dns ptrRec <reverseDomain> show dns ptrRec add dns srvRec <domain> <target> -priority <positive_integer> -weight <positive_integer> -port <positive_integer> rm dns srvRec <domain> set dns srvRec <domain> <target> show dns srvRec [(<domain>) | -type <type>] Done

history

The following operations can be performed on "history":

history

Use this command to see the history of the commands executed on CLI.

Synopsis

history

Example

history 1 add snmp trap SPECIFIC 10.102.130.228 2 save config 3 show system session 4 swhell 5 shell 6 what 7 shell 8 help stat lbvserver ...

man

The following operations can be performed on "man":

man

Use this command to invoke the man page for the specified command.

You can specify the command in full, or partially, if it is uniquely resolvable.

Synopsis

man

Arguments

commandName The name of the command.

Example

man add vs

quit

The following operations can be performed on "quit":

quit

Use this command to terminate the CLI. Note: typing +will also terminate the CLI.

Synopsis

quit

source

The following operations can be performed on "source":

source

Use this command to read the contents of a file and execute each line as a separate CLI command. Each command in the file being read must be on a separate line. Lines starting with # are considered comments.

Synopsis

source <fileName>

Arguments

fileName The name of the file to be sourced.

Example

source cmds.txt

unalias

The following operations can be performed on "unalias":

unalias

Remove an alias

Synopsis

unalias <pattern>

Arguments

pattern Name of the alias

Example

unalias info

whoami

The following operations can be performed on "whoami":

whoami

Show the current user.

Synopsis

whoami

Output

userName loggedIn

cloud

cloud-allowedngsticketprofile

The following operations can be performed on "cloud-allowedngsticketprofile":

add| rm| set| show|

add cloud allowedngsticketprofile

adds allowed ticket profiles

Synopsis

add cloud allowedngsticketprofile <name> -creator <string>

Arguments

name Profile name for allowed tickets

creator Created name for allowed tickets

rm cloud allowedngsticketprofile

removes configured allowed ticket profile

Synopsis

rm cloud allowedngsticketprofile <name>

Arguments

name Name of the allowed ticket profile

set cloud allowedngsticketprofile

Sets any parameter inside allowed ticket profile

Synopsis

set cloud allowedngsticketprofile <name> -creator <string>

Arguments

name Profile name for allowed tickets

creator Created name for allowed tickets

show cloud allowedngsticketprofile

Displays details of the specified allowed ticket profile

Synopsis

show cloud allowedngsticketprofile

Arguments

name Name of the allow ticket profile

Output

creator Created name for allowed tickets

devno count stateflag

cloud-autoscalegroup

The following operations can be performed on "cloud-autoscalegroup":

show cloud autoscalegroup

Displays all autoscale groups configured in this cloud(VPC).

Synopsis

show cloud autoscalegroup

Arguments

name

Output

cloudBuffer Buffer is passed for Python Backend to fill JSON.

azcount Number of Availibility Zone this Autoscale Group is in.

aznames Availibility Zones this Autoscale Group is in.

graceFul Autoscale down policy Set for this Autoscale group

devno count stateflag

Example

An example of the show cloud autoscalegroup command output is as follows: 2 configured Autoscalgroups on this VPC:

cloud-awsParam

The following operations can be performed on "cloud-awsParam":

set| show| unset|

set cloud awsParam

Sets AWS Role ARN for API access

Synopsis

set cloud awsParam -roleARN <string>

Arguments

roleARN IAM Role ARN

show cloud awsParam

Displays AWS Role ARN

Synopsis

show cloud awsParam

Arguments

Output

roleARN IAM Role ARN

unset cloud awsParam

Use this command to remove cloud awsParam settings.Refer to the set cloud awsParam command for meanings of the arguments.

Synopsis

unset cloud awsParam -roleARN

Cloud

The entities on which you can perform NetScaler CLI operations:

- cloud-allowedngsticketprofile
- cloud-autoscalegroup
- cloud-awsParam
- cloud
- cloud-credential
- cloud-ngsparameter
- cloud-paramInternal
- cloud-parameter
- cloud-profile
- cloud-service
- cloud-stats
- cloud-vserverIP

cloud-credential

The following operations can be performed on "cloud-credential":

set| show|

set cloud credential

Sets Cloud credentials for REST API accesses.

Synopsis

set cloud credential -tenantIdentifier <string> -applicationID <string> -applicationSecret

Arguments

tenantIdentifier Tenant ID of the Credentials

applicationID Application ID of the Credentials

applicationSecret Application Secret of the Credentials.

show cloud credential

Displays Cloud credentials

Synopsis

show cloud credential

Arguments

Output

isSet Are the credentials set?

cloud-ngsparameter

The following operations can be performed on "cloud-ngsparameter":

set| show| unset|

set cloud ngsparameter

Synopsis

set cloud ngsparameter

Arguments

blockonallowedngstktprof Enables blocking connections authenticated with a ticket createdby by an entity not whitelisted in allowedngstktprofile

Possible values: YES, NO Default value: NO

allowedudtversion Enables the required UDT version to EDT connections in the CGS deployment

Possible values: V4, V5, V6, V7 Default value: V4

csvserverTicketingDecouple Enables Decoupling CSVSERVER state from Ticketing Service state in the CGS deployment

Possible values: YES, NO Default value: NO

allowdtls12 Enables DTLS1.2 for client connections on CGS

Possible values: YES, NO Default value: NO

show cloud ngsparameter

Synopsis

show cloud ngsparameter

Arguments

Output

blockonallowedngstktprof Enables blocking connections authenticated with a ticket createdby by an entity not whitelisted in allowedngstktprofile

allowedudtversion Enables the required UDT version to EDT connections in the CGS deployment

csvserverTicketingDecouple Enables Decoupling CSVSERVER state from Ticketing Service state in the CGS deployment

allowdtls12 Enables DTLS1.2 for client connections on CGS

unset cloud ngsparameter

Use this command to remove cloud ngsparameter settings.Refer to the set cloud ngsparameter command for meanings of the arguments.

Synopsis

unset cloud ngsparameter

cloud-paramInternal

The following operations can be performed on "cloud-paramInternal":

show| set|

show cloud paramInternal

Displays Citrix ADC internal parameters in context of cloud.

Synopsis

show cloud paramInternal

Arguments

Output

nonftumode Indicates if GUI in in FTU mode or not

iamperm Indicates if user has sufficient IAM previliges

devno count stateflag

set cloud paramInternal

Sets Citrix ADC internal parameters in context of cloud.

Synopsis

set cloud paramInternal

Arguments

nonftumode Indicates if GUI in in FTU mode or not

Possible values: YES, NO

cloud-parameter

The following operations can be performed on "cloud-parameter":

set| unset| show|

set cloud parameter

Set the cloud parameters required to register to the cloud.

Synopsis

set cloud parameter

Arguments

ControllerFQDN FQDN of the controller to which the Citrix ADC SDProxy Connects

ControllerPort Port number of the controller to which the Citrix ADC SDProxy connects Minimum value: 1

InstanceID Instance ID of the customer provided by Trust

CustomerID Customer ID of the citrix cloud customer

ResourceLocation Resource Location of the customer provided by Trust

activationCode Activation code for the NGS Connector instance

Deployment Describes if the customer is a Staging/Production or Dev Citrix Cloud customer

Possible values: Production, Staging, Dev

connectorResidence Identifies whether the connector is located Onprem, Aws or Azure

Possible values: None, Onprem, Aws, Azure, Cpx

unset cloud parameter

Unset the cloud parameters.Refer to the set cloud parameter command for meanings of the arguments.

Synopsis

unset cloud parameter

show cloud parameter

Displays information about cloud parameters

Synopsis

show cloud parameter

Arguments

Output

ControllerFQDN FQDN of the controller to which the Citrix ADC SDProxy Connects

ControllerPort Port number of the controller to which the Citrix ADC SDProxy connects

InstanceID Instance ID of the customer provided by Trust

CustomerID Customer ID of the citrix cloud customer

ResourceLocation Resource Location of the customer provided by Trust

ControlConnectionStatus Status of the control connection: In case of successful registration to the controller, connection status will be shown as "Registered" else "Unregistered".

Deployment Describes if the customer is a Staging/Production or Dev Citrix Cloud customer

connectorResidence Identifies whether the connector is located Onprem, Aws or Azure

cloud-profile

The following operations can be performed on "cloud-profile":

show| rm| add|

show cloud profile

Show cloud profile.

Synopsis

show cloud profile

Arguments

name Name for the Cloud profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the profile is created.

Output

type Type of cloud profile that you want to create, Vserver or based on Azure Tags

vServerName Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver').

serviceType Protocol used by the service (also called the service type).

IPAddress IPv4 or IPv6 address to assign to the virtual server.

port Port number for the virtual server.

serviceGroupName servicegroups bind to this server

boundServiceGroupSvcType The type of bound service

vsvrbindsvcport The port number to be used for the bound service.

azureTagName Azure tag name

azureTagValue Azure tag value

azurePollPeriod Azure polling period (in seconds)

graceFul Indicates graceful shutdown of the service. System will wait for all outstanding connections to this service to be closed before disabling the service.

delay Time, in seconds, after which all the services configured on the server are disabled.

cloudBuffer Buffer is passed for Python Backend to fill JSON.

devno count stateflag

rm cloud profile

Remove cloud profile.

Synopsis

rm cloud profile <name>

Arguments

name Name for the Cloud profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the profile is created.

Output

cloudBuffer Buffer is passed for Python Backend to fill JSON.

add cloud profile

Add cloud profile.

Synopsis

add cloud profile <name> -type (autoscale | azuretags) -vServerName <string> -serviceType <serviceType> -IPAddress <ip_addr|ipv6_addr|> *-port <port|>* -serviceGroupName <string> -boundServiceGroupSvcType <boundServiceGroupSvcType> -vsvrbindsvcport <port|*>

Arguments

name Name for the Cloud profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the profile is created.

type Type of cloud profile that you want to create, Vserver or based on Azure Tags

Possible values: autoscale, azuretags

vServerName Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver').

serviceType Protocol used by the service (also called the service type).

Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, DNS, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, TFTP, ORACLE, SMPP, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, PROXY, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, MONGO, MONGO_TLS, MQTT, MQTT_TLS, QUIC_BRIDGE, HTTP_QUIC

IPAddress IPv4 or IPv6 address to assign to the virtual server.

port Port number for the virtual server.

serviceGroupName servicegroups bind to this server

boundServiceGroupSvcType The type of bound service

Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, ADNS_TCP, MYSQL, MSSQL, ORACLE, MONGO, MONGO_TLS, RADIUS, RADIUSListener,

RDP, DIAMETER, SSL_DIAMETER, TFTP, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, LOGSTREAM_SSL, MQTT, MQTT_TLS, QUIC_BRIDGE

vsvrbindsvcport The port number to be used for the bound service.

graceFul Indicates graceful shutdown of the service. System will wait for all outstanding connections to this service to be closed before disabling the service.

Possible values: YES, NO Default value: NO

delay Time, in seconds, after which all the services configured on the server are disabled.

azureTagName Azure tag name

azureTagValue Azure tag value

azurePollPeriod Azure polling period (in seconds) Default value: 60 Minimum value: 60 Maximum value: 3600

Output

cloudBuffer Buffer is passed for Python Backend to fill JSON.

cloud-service

The following operations can be performed on "cloud-service":

check cloud service

Start the script that tests the connectivity from gateway connector to the NGS Cloud FQDNs

Synopsis

check cloud service

Output

response

cloud-stats

The following operations can be performed on "cloud-stats":

show cloud stats

show cloud stats is an alias for stat cloud

Synopsis

show cloud stats - alias for 'stat cloud'

cloud-vserverIP

The following operations can be performed on "cloud-vserverIP":

show cloud vserverIP

Displays all VIPS on a ENI associated with this instance.

Synopsis

show cloud vserverIP

Arguments

Output

cloudBuffer Buffer is passed for Python Backend to fill JSON.

IPAddress VIPS on a given ENI.

devno count stateflag

Example

An example of the show cloud vserverIPs command output is as follows: 2 configured VIPS: <VIP_IP> <VP_IP>

cloud

The following operations can be performed on "cloud":

stat cloud

Displays the statistics for Citrix Gateway usage.

Synopsis

stat cloud

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

CLXMTP Conn Est time ' 1 sec (NgsShieldLe1secClxmtpConnestTime) Total Connection with CLXMTP connect time less than 1 sec

CLXMTP Conn Est time ' 2 sec (NgsShieldLe2secClxmtpConnestTime) Total Connection with CLXMTP connect time less than 2 sec

CLXMTP Conn Est time ' 3 sec (NgsShieldLe3secClxmtpConnestTime) Total Connection with CLXMTP connect time less than 3 sec

CLXMTP Conn Est time ' 5 sec (NgsShieldLe5secClxmtpConnestTime) Total Connection with CLXMTP connect time less than 5 sec

CLXMTP Conn Est time ' 8 sec (NgsShieldLe8secClxmtpConnestTime) Total Connection with CLXMPT connect time less than 8 sec

CLXMTP Conn Est time ' 13 sec (NgsShieldLe13secClxmtpConnestTime) Total Connection with CLXMPT connect time less than 13 sec

CLXMTP Conn Est time ' 21 sec (NgsShieldLe21secClxmtpConnestTime) Total Connection with CLXMPT connect time less than 21 sec

CLXMTP Conn Est time > 21 sec (NgsShieldGt21secClxmtpConnestTime) Total Connection with CLXMPT connect time greater than 21 sec

GCT Conn Est time ' 1 sec (NgsGctLe1secConnestTime) Total Connection with GCT connect time less than 1 sec

GCT Conn Est time ' 2 sec (NgsGctLe2secConnestTime) Total Connection with GCT connect time less than 2 sec

GCT Conn Est time ' 3 sec (NgsGctLe3secConnestTime) Total Connection with GCT connect time less than 3 sec

GCT Conn Est time ' 5 sec (NgsGctLe5secConnestTime) Total Connection with GCT connect time less than 5 sec

GCT Conn Est time ' 8 sec (NgsGctLe8secConnestTime) Total Connection with GCT connect time less than 8 sec

GCT Conn Est time > 8 sec (NgsGctGt8secConnestTime) Total Connection with GCT connect time greater than 8 sec

CLXMTP Conn Est Attempted (NgsShieldClxmtpConnestAttempted) Total attempted CLXMTP connection

CLXMTP Conn Est Success (NgsShieldClxmtpConnestSuccess) Total successful CLXMTP connection

Toatl CLXMTP Softdeny (NgsShieldClxmtpSoftdeny) Total number of softdeny received by SN

Total CLXMTP Deny (NgsShieldClxmtpDeny) Total number of deny received by SN

Total CLXMTP Allow target (NgsShieldClxmtpAllowtarget) Total number of allowtarget received by SN

Total CLXMTP Redirect target (NgsShieldClxmtpRedirecttarget) Total number of redirecttarget received by SN

Total CLXMTP Connector Fanout Timeout (NgsShieldClxmtpConnectorFanoutTimeout) Total number of fanout timeout

Total CLXMTP Global Fanout Timeout (NgsShieldClxmtpGlobalFanoutTimeout) Total number of global fanout timeout

Total Fanout (NgsShieldFanout) Total number of fanout

Total CL Validation Failure (NgsShieldClValidationFailure) Total Connection lease validation failure

Total CL Decryption Failure (NgsShieldClDecryptionFailure) Total Connection lease decryption failure

Total CLXMTP Complete (NgsShieldClxmtpComplete) Total CLXMTP completed

Total CLXMTP Trust Est Failure (NgsShieldClxmtpTrustestFailure) Total CLXMTP trust establishment failure

Total CLXMTP Pubkey validation Failure (NgsShieldClxmtpPubkeyvalFailure) Total CLXMTP pub key validation failure

Total CLXMTP Conn validation Failure (NgsShieldClxmtpConnvalidationFailure) Total CLXMTP connection lease validation failure

Total CLXMTP Authorize conn req Failure (NgsShieldClxmtpAuthorizeconnreqFailure) Total CLXMTP authorize connection request failure

Total Key Fetch Failure (NgsShieldKeyFetchFailure) Total Shield key fetching failure

Total Demanded Rtkey Not found (NgsShieldDemandedRtkeyNotfound) Total root of trust keys not found failure

Total Demanded Cliskey Not found (NgsShieldDemandedCliskeyNotfound) Total CLIS keys not found failure

Total Demanded Gateway key Notfound (NgsShieldDemandedGwkeyNotfound) Total gateway keys not found failure

Total Key Cache Empty (NgsShieldKeyCacheEmpty) Total shield key cache list empty

Total AKV Get secret list Failure (NgsShieldAkvGetsecretlistFailure) Total failures to get akv secret list

Total AKV Get secret Failure (NgsShieldAkvGetsecretFailure) Total failures to get akv secrets

Total AKV Token Failure (NgsShieldAkvTokenFailure) Total akv token failures

Total AWS Get master secret Failure (NgsShieldAwssmGetmastersecretFailure) Total failures to get aws master secret list

Total AWS Get secret Failure (NgsShieldAwssmGetsecretFailure) Total failures to get aws secrets

Total AWS Token Failure (NgsShieldAwssmTokenFailure) Total aws secret manager token failures

Total V1 Launch Success (NgsRendezvousV1LaunchSuccess) Total rendezvous v1 launch success

Total V1 Launch Failure (NgsRendezvousV1LaunchFailure) Total rendezvous v1 launch failures

Total V2 Launch Success (NgsRendezvousV2LaunchSuccess) Total rendezvous v2 launch success

Total V2 Launch Failure (NgsRendezvousV2LaunchFailure) Total rendezvous v2 launch failures

V1 connect command sent failure (NgsRendezvousV1SntCntCmdFailure) Total rendezvous v1 sent connect command failure

V2 connect command sent failure (NgsRendezvousV2SntCntCmdFailure) Total rendezvous v2 sent connect command failure

V2 to V1 fallback (NgsRendezvousV2FallbackToV1) Total rendezvous v2 to v1 fallback

V2 delayed Response (NgsRendezvousV2DelayedResponse) Total rendezvous v2 delayed response

Invalid Rendezvous Capability (NgsRendezvousV2InvalidCapability) Total invalid rendezvous capability received

NGS Conn Est Time ' 1 sec (NgsLe1secConnestTime) Total connection with NGS connect less than 1 sec

NGS Conn Est Time ' 2 sec (NgsLe2secConnestTime) Total connection with NGS connect less than 2 sec

NGS Conn Est Time ' 3 sec (NgsLe3secConnestTime) Total connection with NGS connect less than 3 sec

NGS Conn Est Time ' 5 sec (NgsLe5secConnestTime) Total connection with NGS connect less than 5 sec

NGS Conn Est Time ' 8 sec (NgsLe8secConnestTime) Total connection with NGS connect less than 8 sec

NGS Conn Est Time > 8 sec (NgsGt8secConnestTime) Total connection with NGS connect greater than 8 sec

Total App Launch Attempted (NgsAppLaunchAttempted) Total app launch attempted

Total App Launch Success (NgsAppLaunchSuccess) Total app launch success

Total App Launch Failure (NgsAppLaunchFailure) Total app launch failures

Total Sta Validation Failure (NgsStaValFailure) Total STA validation failures

Total Sta Validation Success (NgsStaValSuccess) Total STA validation success

Total Ticket Service Down (NgsTicketSvcDown) Total Ticket service down

Total Delayed Connector Response (NgsDelayedConnectorResponse) Total delayed response received from connector

Total Tunnel Closed By Client (NgsTunnelClosedByClient) Total number of tunnels closed by client

Total Tunnel Closed By Vda (NgsTunnelClosedByVda) Total number of tunnels closed by VDA

Total Conn Cmd Fail By Fr (NgsConnCmdFailByFr) Total number fo coonect command failed by FR

Total Conn Cmd Fail Client Conn Notfound (NgsConnCmdFailClientConnNotfound) Totla connect command failed with client connection not found

Total Ica Start (NgsIcaStart) Total number of ICA start

Total Ica End (NgsIcaEnd) Total number of ICA end

Total SOCKS Launch Attempt (NgsSocksAppLaunchAttempted) Total number of SOCKS app launch attempted

Total SOCKS Launch Success (NgsSocksAppLaunchSuccess) Total number of SOCKS app launch success

Total CGP Launch Attempt (NgsCgpAppLaunchAttempted) Total number of CGP app launch attempted

Total CGP Launch Success (NgsCgpAppLaunchSuccess) Total number of CGP app launch success

Total GCT Launch Attempt (NgsGctAppLaunchAttempted) Total number of GCT app launch attempted

Total GCT Launch Success (NgsGctAppLaunchSuccess) Total number of GCT app launch success

Total STA Launch Attempt (NgsStaAppLaunchAttempted) Total number of STA app launch attempted

Total STA Launch Success (NgsStaAppLaunchSuccess) Total number of STA app launch success

EDT Conn Est Time ' 1 sec (NgsEdtLe1secConnestTime) Total EDT connection with connect time less than 1 sec

EDT Conn Est Time ' 2 sec (NgsEdtLe2secConnestTime) Total EDT connection with connect time less than 2 sec

EDT Conn Est Time ' 3 sec (NgsEdtLe3secConnestTime) Total EDT connection with connect time less than 3 sec

EDT Conn Est Time ' 5 sec (NgsEdtLe5secConnestTime) Total EDT connection with connect time less than 5 sec

EDT Conn Est Time ' 8 sec (NgsEdtLe8secConnestTime) Total EDT connection with connect time less than 8 sec

EDT Conn Est Time >= 8 sec (NgsEdtGt8secConnestTime) Total EDT connection with connect time greater than 8 sec

Client Handshake Est Time ' 1s (NgsEdtLe1secClientHandshakeEstTime) Total EDT handshake establishment time with client less than 1sec

Client Handshake Est Time ' 2s (NgsEdtLe2secClientHandshakeEstTime) Total EDT handshake establishment time with client less than 2sec

Client Handshake Est Time ' 3s (NgsEdtLe3secClientHandshakeEstTime) Total EDT handshake establishment time with client less than 3sec

Client Handshake Est Time >= 3s (NgsEdtGt3secClientHandshakeEstTime) Total EDT handshake establishment time with client greater than 3sec

Vda Handshake Est Time ' 1 sec (NgsEdtLe1secVdaHandshakeEstTime) Total EDT handshake establishment time with vda less than 1sec

Vda Handshake Est Time ' 2 sec (NgsEdtLe2secVdaHandshakeEstTime) Total EDT handshake establishment time with vda less than 2sec

Vda Handshake Est Time ' 3 sec (NgsEdtLe3secVdaHandshakeEstTime) Total EDT handshake establishment time with vda less than 3sec

Vda Handshake Est Time >= 3 sec (NgsEdtGt3secVdaHandshakeEstTime) Total EDT handshake establishment time with vda greater than 3sec

EDT Conn Request (NgsEdtConnRequest) Total EDT connection request

EDT Client Conn Est (NgsEdtClientConnest) Total client EDT connection establishment

Conn Req Drop (Non Rendezvous) (NgsEdtNonrendzConnreqDrop) Total connect request drop due to rendezvous not enabled

Send Connect Failure (NgsEdtCtrlSendconnFailure) Total send connect to controller failed

EDT App Launch Success (NgsEdtAppLaunchSuccess) Total EDT app launch success

EDT App Launch Failure (NgsEdtAppLaunchFailure) Total EDT app launch failures

EDT Sta Val Failure (NgsEdtStaValFailure) Total STA validation failures

EDT Sta Val Success (NgsEdtStaValSuccess) Total STA validation success

FR VDA Connection (NgsEdtFrVdaConn) Total FR VDA connection

FR SN Connection (NgsEdtFrSnConn) Total FR SN connection

EDT Vda Conn Est (NgsEdtVdaConnest) Total VDA EDT connection establishment

VDA Rendezvous Timeout (NgsEdtVdaRendezvousTimeout) Total VDA rendezvous timeout

EDT Non Lossy Tunnel (NgsEdtNonLossyTunnel) Total EDT non lossy tunnels

EDT Lossy Tunnel (NgsEdtLossyTunnel) Total EDT lossy tunnels

Redis GET Request (NgsEdtGetrequestSentToRedis) Total Redis GET Request

Redis Lookup Success (NgsEdtRedisLookupSuccess) Total Redis lookup success

Redis Lookup Failure (NgsEdtRedisLookupFailure) Total Redis lookup failure

Redis Entry Addition Success (NgsEdtRedisEntryAddSuccess) Entries Added To Redis Successfully

Redis Entry Addition Success (NgsEdtRedisEntryAddFailure) Entries Addition to Redis failure

Entry Deletion In Redis Successfully (NgsEdtRedisEntryDeleteSuccess) Entry Deleted Successfully In Redis

Entry Deletion In Redis Failure (NgsEdtRedisEntryDeleteFailure) Entry Deletion Failed in Redis

cloudtunnel

Cloudtunnel

The entities on which you can perform NetScaler CLI operations:

- cloudtunnel-parameter
- cloudtunnel-vserver

cloudtunnel-parameter

The following operations can be performed on "cloudtunnel-parameter":

unset| set| show|

unset cloudtunnel parameter

Unset the cloudtunnel parameters.Refer to the set cloudtunnel parameter command for meanings of the arguments.

Synopsis

unset cloudtunnel parameter -SubnetResourceLocationMappings

set cloudtunnel parameter

Synopsis

set cloudtunnel parameter

Arguments

ControllerFQDN fqdn ResourceLocation SubnetResourceLocationMappings

show cloudtunnel parameter

Synopsis

show cloudtunnel parameter

Arguments

Output

ControllerFQDN fqdn ResourceLocation SubnetResourceLocationMappings

cloudtunnel-vserver

The following operations can be performed on "cloudtunnel-vserver":

set| add| show| rm|

set cloudtunnel vserver

Modifies the specified parameters of a Cloud Tunnel virtual server.

Synopsis

set cloudtunnel vserver <name>

Arguments

name Name of the virtual server to modify.

Listenpolicy String specifying the listen policy for the Cloud Tunnel virtual server. Can be either a named expression or an expression. The Cloud Tunnel virtual server processes only the traffic for which the expression evaluates to true. Default value: "none"

Listenpriority Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server, the virtual server whose listen policy has the highest priority (the lowest priority number) accepts the request. Default value: 101 Minimum value: 0 Maximum value: 100

add cloudtunnel vserver

Synopsis

add cloudtunnel vserver <name> <serviceType> [-Listenpolicy <expression>]

Arguments

name Name for the Cloud Tunnel virtual server. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space,colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies

only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my server" or 'my server').

serviceType ServiceType of Listener using which traffic will be tunneled through cloud tunnel server.

Possible values: TCP, UDP

Listenpolicy String specifying the listen policy for the Cloud Tunnel virtual server. Can be either a named expression or an expression. The Cloud Tunnel virtual server processes only the traffic for which the expression evaluates to true. Default value: "none"

Listenpriority Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server, the virtual server whose listen policy has the highest priority (the lowest priority number) accepts the request. Default value: 101 Minimum value: 0 Maximum value: 100

Example

add cloudtunnel vserver tunnel1 TCP

show cloudtunnel vserver

Displays information about Cloud Tunnel vserver.

Synopsis

show cloudtunnel vserver

Arguments

name Name of cloud tunnel vserver

Output

serviceType ServiceType of Listener using which traffic will be tunneled through cloud tunnel server.

state The current state of the virtual server, as UP, DOWN, BUSY, and so on.

effectiveState type The type of virtual server; for example, CONTENT based or ADDRESS based.

IPAddress The Virtual IP address of the Cloud Tunnel virtual server.

IPAddress IPv4 or IPv6 address of the Cloud Tunnel virtual server.

IPPattern The IP pattern of the virtual server.

port Port on which the virtual server listens.

range cacheType Virtual server cache type. The options are: TRANSPARENT, REVERSE, and FORWARD.

Listenpolicy String specifying the listen policy for the Cloud Tunnel virtual server. Can be either a named expression or an expression. The Cloud Tunnel virtual server processes only the traffic for which the expression evaluates to true.

Listenpriority Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server, the virtual server whose listen policy has the highest priority (the lowest priority number) accepts the request.

devno count stateflag

rm cloudtunnel vserver

Removes a configured cloudtunnel virtual server.

Synopsis

rm cloudtunnel vserver <name>@ ...

Arguments

name Name of the virtual server to remove.

Example

rm cloudtunnel vserver tunnel1

cluster

Cluster

The entities on which you can perform NetScaler CLI operations:

- cluster
- cluster-files
- cluster-instance
- cluster-node
- cluster-nodegroup
- cluster-propstatus
- cluster-sync
- cluster-syncFailures

cluster-files

The following operations can be performed on "cluster-files":

sync cluster files

Synchronizes SSL Certificates, SSL CRL lists, SSL VPN bookmarks, and other files from the configuration coordinator (CCO) to the other cluster nodes. Execute this command from the cluster IP address only. This command is automatically triggered from the CCO when a new node is added to a cluster and periodically triggered to synchronize updated files between the cluster nodes. Note: Files on non-CCO nodes are not deleted if they do no not exist on the CCO.

Synopsis

sync cluster files

Arguments

Mode The directories and files to be synchronized. The available settings function as follows: Mode Paths all /nsconfig/ssl/ /var/netscaler/ssl/ /var/vpn/bookmark/ /nsconfig/dns/ /nsconfig/

monitors/ /nsconfig/nstemplates/ /nsconfig/ssh/ /nsconfig/rc.netscaler /nsconfig/resolv.conf / nsconfig/inetd.conf /nsconfig/syslog.conf /nsconfig/ntp.conf /nsconfig/httpd.conf /nsconfig/ sshd_config /nsconfig/hosts /nsconfig/enckey /var/nslw.bin/etc/krb5.conf /var/nslw.bin/etc/ krb5.keytab /var/lib/likewise/db/ /var/download/ /var/wi/tomcat/webapps/ /var/wi/tomcat/conf/ Catalina/localhost/ /var/wi/java_home/lib/security/cacerts /var/wi/java_home/jre/lib/security/cacerts / var/netscaler/locdb/ ssl /nsconfig/ssl/ /var/netscaler/ssl/ bookmarks /var/vpn/bookmark/ dns / nsconfig/dns/ imports /var/download/ misc /nsconfig/license/ /nsconfig/rc.conf all_plus_misc Includes *all* files and /nsconfig/license/ and /nsconfig/rc.conf. Default value: all

Example

sync cluster files ssl or sync cluster files all

cluster-instance

The following operations can be performed on "cluster-instance":

stat| enable| show| unset| set| add| disable| rm|

stat cluster instance

Displays statistics for a cluster instance.

Synopsis

stat cluster instance

Arguments

clId ID of the cluster instance for which to display statistics. Minimum value: 1 Maximum value: 16

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Traffic transmitted (Bkplane Tx) Traffic transmitted from backplane (in mbits)

Traffic received (Bkplane Rx) Traffic received on backplane (in mbits)

Cluster size (CLNumNodes) Number of nodes in the cluster.

Cluster status (CLCurEnable) State of the cluster.

Configuration coordinator (CLViewLeader) NSIP address of the Configuration Coordinator of the cluster.

Total steered packets (TotSteeredPkts) Total number of packets steered on the cluster backplane.

Dropped steered packets (DFDdropPkts) Number of steered packets that are dropped.

Propagation timeout (propTimeout) Number of times the update to the client timed-out.

Related Commands

- stat cluster node

enable cluster instance

Enables a cluster instance.

Synopsis

enable cluster instance <clId>

Arguments

clId ID of the cluster instance that you want to enable. Minimum value: 1 Maximum value: 16

Example

enable cluster instance 1

show cluster instance

Displays information about the cluster instance and its nodes.

Synopsis

show cluster instance

Arguments

clId Unique number that identifies the cluster. Minimum value: 1 Maximum value: 16

Output

deadInterval Amount of time, in seconds, after which nodes that do not respond to the heartbeats are assumed to be down.If the value is less than 3 sec, set the helloInterval parameter to 200 msec

helloInterval Interval, in milliseconds, at which heartbeats are sent to each cluster node to check the health status.Set the value to 200 msec, if the deadInterval parameter is less than 3 sec

preemption Preempt a cluster node that is configured as a SPARE if an ACTIVE node becomes available.

adminstate Cluster Admin State.

quorumType Quorum Configuration Choices - "Majority" (recommended) requires majority of nodes to be online for the cluster to be UP. "None" relaxes this requirement.

propState Enable/Disable the execution of commands on the cluster. This will not impact the execution of commands on individual cluster nodes by using the NSIP.

inc This option is required if the cluster nodes reside on different networks.

nodegroup The node group in a Cluster system used for transition from L2 to L3.

processLocal By turning on this option packets destined to a service in a cluster will not under go any steering.

validMtu Correct MTU value that has to be set on backplane.

retainConnectionsOnCluster This option enables you to retain existing connections on a node joining a Cluster system or when a node is being configured for passive timeout. By default, this option is disabled.

heterogeneousFlag This field diplay if heterogeneous is detected in the cluster system.

backplaneBasedView View based on heartbeat only on bkplane interface

syncStatusStrictMode strict mode for sync status of cluster. Depending on the the mode if there are any errors while applying config, sync status is displayed accordingly. By default the flag is disabled.

dfdretainl2params flag to add ext l2 header during steering. By default the flag is disabled.

clusterProxyArp This field controls the proxy arp feature in cluster. By default the flag is enabled.

nodeId The unique number that identiies a cluster.

IPAddress The IP Address of the node.

flags The flags for this entry.

masterState Master state.

health Node Health state.

clusterHealth Node clusterd state.

effectiveState Node effective health state.

state Active, Spare or Passive. An active node serves traffic. A spare node serves as a backup for active nodes. A passive node does not serve traffic. This may be useful during temporary maintenance activity where it is desirable that the node takes part in the consensus protocol, but not serve traffic.

flag Cluster Flag.

operationalstate Cluster Operational State.

status Cluster Operational State.

isConfigurationCoordinator This argument is used to determine whether the node is configuration coordinator (CCO).

isLocalnode This argument is used to determine whether it is local node.

RSSKeyMismatch This argument is used to determine if there is a RSS key mismatch at cluster instance level.

PENumMismatch This argument is used to determine if there is a PE number mismatch at cluster instance level.

NodegroupStateWarning This argumnt is used to determind whether all the cluster nodes are bound to nodegroup with state set.

LicenseMismatch This argument is used to determine if there is a License mismatch at cluster instance level.

JumboNotSupported This argument is used to determine if Jumbo framework is not supported at cluster instance level.

ClusterNoHeartbeatOnNode HB is not seen on the backplane interface of member node

ClusterNoLinksetMBF MBF is enabled but linkset is not configured

ClusterNoSpottedIp There is no spotted SNIP or MIP

NodeRSSKeyMismatch This argument is used to determine if there is a RSS key mismatch at cluster node level.

NodePENumMismatch This argument is used to determine if there is a PE missmatch at cluster node level.

NodeLicenseMismatch This argument is used to determine if there is a License mismatch at cluster node level.

NodeJumboNotSupported This argument is used to determine if Jumbo framework not supported at cluster node level.

stateflag State Flag.

operationalPropState Cluster Operational Propagation State.

devno count

Example

An example of the command's output is as follows: 1)Cluster ID: 1 Dead Interval: 3 secs Hello Interval: 200 msecs Preemption: DISABLED Propagation: ENABLED Cluster Status: ENABLED(admin), ENABLED(operational), UP Member Nodes: Node ID Node IP Health Admin State Operational State

1.
```
1               1.1.1.1*             UP         ACTIVE
 ACTIVE(Configuration Coordinator)
```

2.
```
2               1.1.1.2             UP          ACTIVE
 ACTIVE
```

Done *: Local node

unset cluster instance

Use this command to remove cluster instance settings.Refer to the set cluster instance command for meanings of the arguments.

Synopsis

unset cluster instance <clId>

set cluster instance

Modifies the specified attributes of a cluster instance.

Synopsis

set cluster instance <clId>

Arguments

clId ID of the cluster instance to be modified. Minimum value: 1 Maximum value: 16

deadInterval Amount of time, in seconds, after which nodes that do not respond to the heartbeats are assumed to be down.If the value is less than 3 sec, set the helloInterval parameter to 200 msec Default value: 3 Minimum value: 1 Maximum value: 60

helloInterval Interval, in milliseconds, at which heartbeats are sent to each cluster node to check the health status.Set the value to 200 msec, if the deadInterval parameter is less than 3 sec Default value: 200 Minimum value: 200 Maximum value: 1000

preemption Preempt a cluster node that is configured as a SPARE if an ACTIVE node becomes available.

Possible values: ENABLED, DISABLED Default value: DISABLED

quorumType Quorum Configuration Choices - "Majority" (recommended) requires majority of nodes to be online for the cluster to be UP. "None" relaxes this requirement.

Possible values: MAJORITY, NONE Default value: MAJORITY

inc This option is required if the cluster nodes reside on different networks.

Possible values: ENABLED, DISABLED Default value: DISABLED

processLocal By turning on this option packets destined to a service in a cluster will not under go any steering.

Possible values: ENABLED, DISABLED Default value: DISABLED

nodegroup The node group in a Cluster system used for transition from L2 to L3.

retainConnectionsOnCluster This option enables you to retain existing connections on a node joining a Cluster system or when a node is being configured for passive timeout. By default, this option is disabled.

Possible values: YES, NO Default value: NO

backplaneBasedView View based on heartbeat only on bkplane interface

Possible values: ENABLED, DISABLED Default value: DISABLED

syncStatusStrictMode strict mode for sync status of cluster. Depending on the the mode if there are any errors while applying config, sync status is displayed accordingly. By default the flag is disabled.

Possible values: ENABLED, DISABLED Default value: DISABLED

dfdretainl2params flag to add ext l2 header during steering. By default the flag is disabled.

Possible values: ENABLED, DISABLED Default value: DISABLED

clusterProxyArp This field controls the proxy arp feature in cluster. By default the flag is enabled.

Possible values: ENABLED, DISABLED Default value: ENABLED

Example

set cluster instance 1 -preemption ENABLED

add cluster instance

Adds a cluster instance to the appliance. Execute this command on only the first node that you add to the cluster.

Synopsis

add cluster instance <clId>

Arguments

clId Unique number that identifies the cluster. Minimum value: 1 Maximum value: 16

deadInterval Amount of time, in seconds, after which nodes that do not respond to the heartbeats are assumed to be down.If the value is less than 3 sec, set the helloInterval parameter to 200 msec Default value: 3 Minimum value: 1 Maximum value: 60

helloInterval Interval, in milliseconds, at which heartbeats are sent to each cluster node to check the health status.Set the value to 200 msec, if the deadInterval parameter is less than 3 sec Default value: 200 Minimum value: 200 Maximum value: 1000

preemption Preempt a cluster node that is configured as a SPARE if an ACTIVE node becomes available.

Possible values: ENABLED, DISABLED Default value: DISABLED

quorumType Quorum Configuration Choices - "Majority" (recommended) requires majority of nodes to be online for the cluster to be UP. "None" relaxes this requirement.

Possible values: MAJORITY, NONE Default value: MAJORITY

inc This option is required if the cluster nodes reside on different networks.

Possible values: ENABLED, DISABLED Default value: DISABLED

processLocal By turning on this option packets destined to a service in a cluster will not under go any steering.

Possible values: ENABLED, DISABLED Default value: DISABLED

retainConnectionsOnCluster This option enables you to retain existing connections on a node joining a Cluster system or when a node is being configured for passive timeout. By default, this option is disabled.

Possible values: YES, NO Default value: NO

backplaneBasedView View based on heartbeat only on bkplane interface

Possible values: ENABLED, DISABLED Default value: DISABLED

syncStatusStrictMode strict mode for sync status of cluster. Depending on the the mode if there are any errors while applying config, sync status is displayed accordingly. By default the flag is disabled.

Possible values: ENABLED, DISABLED Default value: DISABLED

dfdretainl2params flag to add ext l2 header during steering. By default the flag is disabled.

Possible values: ENABLED, DISABLED Default value: DISABLED

clusterProxyArp This field controls the proxy arp feature in cluster. By default the flag is enabled.

Possible values: ENABLED, DISABLED Default value: ENABLED

Example

add cluster instance 1

disable cluster instance

Disables a cluster instance.

Synopsis

disable cluster instance <clId>

Arguments

clId ID of the cluster instance that you want to disable. Minimum value: 1 Maximum value: 16

Example

disable cluster instance 1

rm cluster instance

Removes the cluster instance from the node. You must execute this command on the Citrix ADC IP (NSIP) address of the node.

Synopsis

rm cluster instance <clId>

Arguments

clId Unique number that identifies the cluster. Minimum value: 1 Maximum value: 16

Example

rm cluster instance 1

cluster-node

The following operations can be performed on "cluster-node":

set| show| unset| rm| unbind| bind| add| stat|

set cluster node

Modifies the attributes of a cluster node.

Synopsis

set cluster node <nodeId>@

Arguments

nodeId ID of the cluster node to be modified. Minimum value: 0 Maximum value: 31

state Admin state of the cluster node. The available settings function as follows: ACTIVE - The node serves traffic. SPARE - The node does not serve traffic unless an ACTIVE node goes down. PASSIVE - The node does not serve traffic, unless you change its state. PASSIVE state is useful during temporary maintenance activities in which you want the node to take part in the consensus protocol but not to serve traffic.

Possible values: ACTIVE, SPARE, PASSIVE Default value: PASSIVE

backplane Interface through which the node communicates with the other nodes in the cluster. Must be specified in the three-tuple form n/c/u, where n represents the node ID and c/u refers to the interface on the appliance. Minimum value: 1

priority Preference for selecting a node as the configuration coordinator. The node with the lowest priority value is selected as the configuration coordinator. When the current configuration coordinator goes down, the node with the next lowest priority is made the new configuration coordinator. When the original node comes back up, it will preempt the new configuration coordinator and take over as the configuration coordinator. Note: When priority is not configured for any of the nodes or if multiple nodes have the same priority, the cluster elects one of the nodes as the configuration coordinator. Default value: 31 Minimum value: 0 Maximum value: 31

delay Applicable for Passive node and node becomes passive after this timeout (in minutes) Default value: 0 Maximum value: 1440

tunnelmode To set the tunnel mode

Possible values: NONE, GRE, UDP Default value: NONE

Example

set cluster node 1 -state PASSIVE

show cluster node

Displays information about the cluster node.

Synopsis

show cluster node

Arguments

nodeId ID of the cluster node for which to display information. If an ID is not provided, information about all nodes is shown. Default value: 255 Minimum value: 0 Maximum value: 31

Output

IPAddress The IP Address of the node.

flags The flags for this entry.

clusterHealth Node clusterd state.

effectiveState Node effective health state.

operationalSyncState Node Operational Reconciliation state.

syncFailureReason Displays the additional information along with cluster sync status

masterState Node Master state.

health Node Health state.

state Active, Spare or Passive.

backplane Interface through which the node communicates with the other nodes in the cluster. Must be specified in the three-tuple form n/c/u, where n represents the node ID and c/u refers to the interface on the appliance.

syncState Enable/Disable the synchronization of cluster configurations on the node.

priority Preference for selecting a node as the configuration coordinator. The node with the lowest priority value is selected as the configuration coordinator. When the current configuration coordinator goes down, the node with the next lowest priority is made the new configuration coordinator. When the original node comes back up, it will preempt the new configuration coordinator and take over as the configuration coordinator. Note: When priority is not configured for any of the nodes or if multiple nodes have the same priority, the cluster elects one of the nodes as the configuration coordinator.

isConfigurationCoordinator This argument is used to determine whether the node is configuration coordinator (CCO).

isLocalnode This argument is used to determine whether it is local node.

NodeRSSKeyMismatch This argument is used to determine if there is a RSS key mismatch at cluster node level.

NodeLicenseMismatch This argument is used to determine if there is a License mismatch at cluster node level.

NodeJumboNotSupported This argument is used to determine if Jumbo framework not supported at cluster node level.

stateflag nodeList Nodelist for displaying Heartbeat not seen interfaces on a cluster node

ifacesList Interface list corresponding to nodelist for Heartbeat not seen interfaces on a cluster node

enabledIfaces Enabled Interfaces on a cluster node.

disabledIfaces Disabled Interfaces on a cluster node.

partialFailIfaces Partial Failure Interfaces on a cluster node.

hamonIfaces Hamon Interfaces on a cluster node.

ifaces Interfaces status on cluster node.

nodegroup The default node group in a Cluster system.

name Name of the state specific nodegroup.

cfgflags Flag indicates whether the node is bound to cluster nodegroup

routeMonitor The IP address (IPv4 or IPv6).

routeMonState Current routemonstate

netmask The netmask.

delay Applicable for Passive node and node becomes passive after this timeout (in minutes)

curPassiveTimeout Applicable for Passive node and node becomes passive after this timeout

isLearnedAsPassive Applicable for Active nodes, it will be set to TRUE if the node is active but learned as Passive

tunnelmode To set the tunnel mode

devno count

Example

An example of the command's output is as follows: 1 cluster node: 1)Node ID: 1 IP: 1.1.1.1* Backplane: 1/1/1 Health: UP Admin State: ACTIVE Operational State: ACTIVE(Configuration Coordinator) Sync State: DISABLED Done *: Local node

unset cluster node

Use this command to remove cluster node settings.Refer to the set cluster node command for meanings of the arguments.

Synopsis

unset cluster node <nodeId>@

rm cluster node

Removes a node from the cluster and removes the cluster instance from the node. You must execute this command on the cluster IP address.

Synopsis

rm cluster node <nodeId>

Arguments

nodeId ID of the cluster node to be removed from the cluster. Minimum value: 0 Maximum value: 31

clearNodegroupConfig Option to remove nodegroup config

Possible values: YES, NO Default value: YES

Example

rm cluster node 1

unbind cluster node

Removes a route monitor entry from the local node

Synopsis

unbind cluster node <nodeId> (-routeMonitor <ip_addr|ipv6_addr|*>)

Arguments

nodeId A number that uniquely identifies the cluster node. Minimum value: 0 Maximum value: 31

routeMonitor Route Monitor

netmask The subnet mask associated with the IPv4 route specified by the routeMonitor parameter.

Example

unbind cluster node 1 -routeMonitor 5.5.5.0 255.255.255.0

bind cluster node

Adds a route monitor to the specified cluster node.

Synopsis

bind cluster node <nodeId> (-routeMonitor <ip_addr|ipv6_addr|*>)

Arguments

nodeId A number that uniquely identifies the cluster node. Minimum value: 0 Maximum value: 31

routeMonitor Route Monitor

netmask The subnet mask associated with the IPv4 route specified by the routeMonitor parameter.

Example

bind cluster node 1 -routeMonitor 5.5.5.0 255.255.255.0

add cluster node

Adds a Citrix ADC to a cluster.

Synopsis

add cluster node <nodeId>@ <IPAddress>@

Arguments

nodeId Unique number that identifies the cluster node. Minimum value: 0 Maximum value: 31

IPAddress Citrix ADC IP (NSIP) address of the appliance to add to the cluster. Must be an IPv4 address.

state Admin state of the cluster node. The available settings function as follows: ACTIVE - The node serves traffic. SPARE - The node does not serve traffic unless an ACTIVE node goes down. PASSIVE - The node does not serve traffic, unless you change its state. PASSIVE state is useful during temporary maintenance activities in which you want the node to take part in the consensus protocol but not to serve traffic.

Possible values: ACTIVE, SPARE, PASSIVE Default value: PASSIVE

backplane Interface through which the node communicates with the other nodes in the cluster. Must be specified in the three-tuple form n/c/u, where n represents the node ID and c/u refers to the interface on the appliance. Minimum value: 1

priority Preference for selecting a node as the configuration coordinator. The node with the lowest priority value is selected as the configuration coordinator. When the current configuration coordinator goes down, the node with the next lowest priority is made the new configuration coordinator. When the original node comes back up, it will preempt the new configuration coordinator and take over as the configuration coordinator. Note: When priority is not configured for any of the nodes or if multiple nodes have the same priority, the cluster elects one of the nodes as the configuration coordinator. Default value: 31 Minimum value: 0 Maximum value: 31

nodegroup The default node group in a Cluster system. Default value: DEFAULT_NG

delay Applicable for Passive node and node becomes passive after this timeout (in minutes) Default value: 0 Maximum value: 1440

tunnelmode To set the tunnel mode

Possible values: NONE, GRE, UDP Default value: NONE

Example

add cluster node 1 1.1.1.1 -backplane 1/1/1 -state ACTIVE

stat cluster node

Displays statistics for a cluster node.

Synopsis

stat cluster node

Arguments

nodeId ID of the cluster node for which to display statistics. If an ID is not provided, statistics are shown for all nodes. Minimum value: 0 Maximum value: 31

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Sync state (Sync State) Sync state of the cluster node.

Health Health of the cluster node.

Node IP (NodeIP) NSIP address of the cluster node.

Operational state (OpState) Operational state of the cluster node.

Heartbeats transmitted (HB Sent) Number of heartbeats sent. When executed from the NSIP address, shows the statistics for local node only. For remote node it shows a value of 0. When executed from the cluster IP address, shows all the statistics.

Heartbeats received (HB Rcvd) Number of heartbeats received. When executed from the NSIP address, shows the statistics for local node only. For remote node it shows a value of 0. When executed from the cluster IP address, shows all the statistics.

Current node-node connections (NNMCurConn) Number of connections open for node-to-node communication.

Node-node messages transmitted (NNMTotConnTx) Number of node-to-node messages sent. When executed from the NSIP address, shows the statistics for local node only. For remote node it shows a value of 0. When executed from the cluster IP address, shows all the statistics.

Node-node messages received (NNMTotConnRx) Number of node-to-node messages received. When executed from the NSIP address, shows the statistics for local node only. For remote node it shows a value of 0. When executed from the cluster IP address, shows all the statistics.

PTP operational state (PTP State) PTP state of the node. This state is Master for one node and Slave for the rest. When executed from the NSIP address, shows the statistics for local node only. For remote node it shows UNKNOWN. When executed from the cluster IP address, shows all the statistics.

PTP packets transmitted (PTP Tx) Number of PTP packets transmitted by the node. When executed from the NSIP address, shows the statistics for local node only. For remote node it shows a value of 0. When executed from the cluster IP address, shows all the statistics.

PTP packets received (PTP Rx) Number of PTP packets received on the node. When executed from the NSIP address, shows the statistics for local node only. For remote node it shows a value of 0. When executed from the cluster IP address, shows all the statistics.

Multicast/Broadcast send errors (NNMErrMsend) Number of errors in sending node-to-node multicast/broadcast messages. When executed from the NSIP address, shows the statistics for local node only. For remote node it shows a value of 0. When executed from the cluster IP address, shows all the statistics.

(Health) Health of the node in the cluster.

CH State Health State of the node with respect to sync in the cluster.

Sync state (Sync State) Sync state of the cluster node.

Related Commands

- stat cluster instance

cluster-nodegroup

The following operations can be performed on "cluster-nodegroup":

show| unbind| bind| set| add| rm| unset|

show cluster nodegroup

Displays information about the available nodegroups.

Synopsis

show cluster nodegroup

Arguments

name Name of the nodegroup to be displayed. If a name is not provided, information about all nodegroups is displayed.

Output

node Nodes in the nodegroup

strict Specifies whether cluster nodes, that are not part of the nodegroup, will be used as backup for the nodegroup.

- Enabled - When one of the nodes goes down, no other cluster node is picked up to replace it. When the node comes up, it will continue being part of the nodegroup.
- Disabled - When one of the nodes goes down, a non-nodegroup cluster node is picked up and acts as part of the nodegroup. When the original node of the nodegroup comes up, the backup node will be replaced.

sticky Only one node can be bound to nodegroup with this option enabled. It specifies whether to prempt the traffic for the entities bound to nodegroup when owner node goes down and rejoins the cluster.

- Enabled - When owner node goes down, backup node will become the owner node and takes the traffic for the entities bound to the nodegroup. When bound node rejoins the cluster, traffic for the entities bound to nodegroup will not be steered back to this bound node. Current owner will have the ownership till it goes down.

- Disabled - When one of the nodes goes down, a non-nodegroup cluster node is picked up and acts as part of the nodegroup. When the original node of the nodegroup comes up, the backup node will be replaced.

vServer vserver that need to be bound to this nodegroup.

currentNodeMask Bitmap of current nodes in this nodegroup

backupNodeMask Bitmap of backup nodes in this nodegroup

boundedEntitiesCntFromPE Count of bounded entities to this nodegroup accoding to PE

boundedConfigEntitiesCnt Number of configs bound to this nodegroup

activeList Active node list of this nodegroup

backupList Backup node list of this nodegroup

identifierName stream identifier and rate limit identifier that need to be bound to this nodegroup.

gslbSite vserver that need to be bound to this nodegroup.

service name of the service bound to this nodegroup.

stateflag cfgflags This contains the flags for Cluster Nodegroup in DB

state State of the nodegroup. All the nodes binding to this nodegroup must have the same state. ACTIVE/SPARE/PASSIVE

priority Priority of Nodegroup. This priority is used for all the nodes bound to the nodegroup for Nodegroup selection

devno count

unbind cluster nodegroup

Unbinds a cluster node or an entity from a given nodegroup.

Synopsis

unbind cluster nodegroup <name> (-node <positive_integer>@ | -vServer <string> | -identifierName <string> | -gslbSite <string> | -service <string>)

Arguments

name Name of the nodegroup from which you want to unbind a cluster node or an entity.

node ID of the node to be unbound from the nodegroup. Default value: -1 Minimum value: 0 Maximum value: 31

vServer Name of the virtual server to be unbound from the nodegroup.

identifierName Name of stream or limit identifier to be unbound from the nodegroup.

gslbSite Name of the GSLB site to be unbound from the nodegroup.

service Name of the service to be unbound from the nodegroup.

Example

unbind cluster nodegroup ng1 -vserver v1

bind cluster nodegroup

Binds a cluster node or an entity to the given nodegroup. A node can be bound to more than one nodegroup.

Synopsis

bind cluster nodegroup <name> (-node <positive_integer>@ | -vServer <string> | -identifierName <string> | -gslbSite <string> | -service <string>)

Arguments

name Name of the nodegroup to which you want to bind a cluster node or an entity.

node ID of the node to be bound to the nodegroup. Default value: -1 Minimum value: 0 Maximum value: 31

vServer Name of the virtual server to be bound to the nodegroup.

identifierName Name of stream or limit identifier to be bound to the nodegroup.

gslbSite Name of the GSLB site to be associated with the nodegroup.

service Name of the ADNS or ADNS-TCP service to be associated with the nodegroup. This parameter is used to support GSLB in a cluster.

Example

bind cluster nodegroup ng1 -vserver v1

set cluster nodegroup

Modifies the attributes of a cluster nodegroup.

Synopsis

set cluster nodegroup <name>@

Arguments

name Name of the nodegroup to be modified.

strict Specifies whether cluster nodes, that are not part of the nodegroup, will be used as backup for the nodegroup.

- Enabled - When one of the nodes goes down, no other cluster node is picked up to replace it. When the node comes up, it will continue being part of the nodegroup.
- Disabled - When one of the nodes goes down, a non-nodegroup cluster node is picked up and acts as part of the nodegroup. When the original node of the nodegroup comes up, the backup node will be replaced.

Possible values: YES, NO Default value: NO

state State of the nodegroup. All the nodes binding to this nodegroup must have the same state. ACTIVE/SPARE/PASSIVE

Possible values: ACTIVE, SPARE, PASSIVE Default value: VAL_NOT_SET

priority Priority of Nodegroup. This priority is used for all the nodes bound to the nodegroup for Nodegroup selection Default value: -1 Minimum value: 0 Maximum value: 31

Example

set cluster nodegroup ng1 -strict yes

add cluster nodegroup

Adds a nodegroup to the cluster. A nodegroup is a set of cluster nodes to which entities can be bound. Entities that are bound to a specific nodegroup are active on all the nodes of the group and not active on the nodes that are not part of the group.

Synopsis

add cluster nodegroup <name>@

Arguments

name Name of the nodegroup. The name uniquely identifies the nodegroup on the cluster.

strict Specifies whether cluster nodes, that are not part of the nodegroup, will be used as backup for the nodegroup.

- Enabled - When one of the nodes goes down, no other cluster node is picked up to replace it. When the node comes up, it will continue being part of the nodegroup.
- Disabled - When one of the nodes goes down, a non-nodegroup cluster node is picked up and acts as part of the nodegroup. When the original node of the nodegroup comes up, the backup node will be replaced.

Possible values: YES, NO Default value: NO

sticky Only one node can be bound to nodegroup with this option enabled. It specifies whether to prempt the traffic for the entities bound to nodegroup when owner node goes down and rejoins the cluster.

- Enabled - When owner node goes down, backup node will become the owner node and takes the traffic for the entities bound to the nodegroup. When bound node rejoins the cluster, traffic for the entities bound to nodegroup will not be steered back to this bound node. Current owner will have the ownership till it goes down.
- Disabled - When one of the nodes goes down, a non-nodegroup cluster node is picked up and acts as part of the nodegroup. When the original node of the nodegroup comes up, the backup node will be replaced.

Possible values: YES, NO Default value: NO

state State of the nodegroup. All the nodes binding to this nodegroup must have the same state. ACTIVE/SPARE/PASSIVE

Possible values: ACTIVE, SPARE, PASSIVE Default value: VAL_NOT_SET

priority Priority of Nodegroup. This priority is used for all the nodes bound to the nodegroup for Nodegroup selection Default value: -1 Minimum value: 0 Maximum value: 31

Example

add cluster nodegroup ng1 -strict yes

rm cluster nodegroup

Removes a nodegroup from the cluster.

Synopsis

rm cluster nodegroup <name>@

Arguments

name Name of the nodegroup to be removed.

Example

rm cluster nodegroup ng1

unset cluster nodegroup

Unset nodes from the given nodegroup or unset strict option.Refer to the set cluster nodegroup command for meanings of the arguments.

Synopsis

unset cluster nodegroup <name>@

Example

unset cluster nodegroup ng1 -strict

cluster-propstatus

The following operations can be performed on "cluster-propstatus":

show| clear|

show cluster propstatus

Gets the cluster propagation status

Synopsis

show cluster propstatus

Arguments

Output

NumPropCmdFailed Number of propogated comands failed on this node.

CmdStrs devno count stateflag

Example

show cluster propstatus

clear cluster propstatus

Clears the cluster propagation status, works only on CLIP

Synopsis

clear cluster propstatus

Example

clear cluster propstatus

cluster-sync

The following operations can be performed on "cluster-sync":

force cluster sync

Synchronize the configurations of a cluster node from the configuration coordinator (CCO). This command must be executed from the NSIP of the node that is to be synchronized.

Synopsis

force cluster sync

Arguments

Example

force cluster sync

cluster-syncFailures

The following operations can be performed on "cluster-syncFailures":

show cluster syncFailures

Displays the command execution failures occurred during Cluster Configuration Synchronization.

Synopsis

show cluster syncFailures

Example

show cluster syncFailures

cluster

The following operations can be performed on "cluster":

join cluster

Joins the appliance to the cluster. You must execute this command from the Citrix ADC IP (NSIP) address of the node that you want to add to the cluster. This command is the second part of the two-step process of adding a cluster node. The first part is adding this node to the cluster by using the add cluster node command from the cluster IP address. This operation is not permitted if any node in the cluster is in the Sync state.

Synopsis

join cluster -clip <ip_addr> {-password }

Arguments

clip Cluster IP address to which to add the node.

password Password for the nsroot account of the configuration coordinator (CCO).

cmp

cmp-action

The following operations can be performed on "cmp-action":

rename| unset| show| set| add| rm|

rename cmp action

Renames a compression action.

Synopsis

rename cmp action <name>@ <newName>@

Arguments

name Existing name of the action.

newName New name for the compression action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Choose a name that can be correlated with the function that the action performs.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cmp action" or 'my cmp action').

Example

rename cmp policy oldname newname

unset cmp action

Use this command to remove cmp action settings.Refer to the set cmp action command for meanings of the arguments.

Synopsis

unset cmp action <name> -addVaryHeader

show cmp action

Displays information about all the built-in and user-defined compression actions, or detailed information about the specified action.

Synopsis

show cmp action

Arguments

name Name of the action for which to display detailed information.

Output

cmpType Type of compression performed by this action. Available settings function as follows:

- COMPRESS - Apply GZIP or DEFLATE compression to the response, depending on the request header. Prefer GZIP.
- GZIP - Apply GZIP compression.
- DEFLATE - Apply DEFLATE compression.
- NOCOMPRESS - Do not compress the response if the request matches a policy that uses this action.

deltaType The type of delta action if compression type is delta compression.

addVaryHeader Control insertion of the Vary header in HTTP responses compressed by Citrix ADC. Intermediate caches store different versions of the response for different values of the headers present in the Vary response header.

varyHeaderValue The value of the HTTP Vary header for compressed responses.

stateflag flags builtin Flag to determine whether compression is default or not

feature The feature to be checked while applying this config

isDefault A value of true is returned if it is a default policy

devno count

Example

Example 1

The following example shows output from the show cmp action command when no custom cmp actions have been defined:

```
show cmp action 3 Compression actions:
```

1. ```
   Name: GZIP      Compression Type: gzip
   ```
2. ```
   Name: NOCOMPRESS        Compression Type: nocompress
   ```
3. ```
   Name: DEFLATE   Compression Type: deflate
   ```
4. ```
   Name: COMPRESS  Compression Type: compress
   ```

Done

Done Example 2 The following command creates a compression action: add cmp action nocmp NOCOMPRESS The following example shows output from the show cmp action command after the previous command has been issued:

```
show cmp action 3 Compression actions:
```

1. ```
   Name: GZIP      Compression Type: gzip
   ```
2. ```
   Name: NOCOMPRESS        Compression Type: nocompress
   ```
3. ```
   Name: DEFLATE   Compression Type: deflate
   ```
4. ```
    Name: COMPRESS  Compression Type: compress



   1 Compression action:
   ```

5. ```
   Name: nocmp     Compression Type: nocompress
   ```

Done

set cmp action

Modifies the specified parameters of a compression action.

Synopsis

set cmp action <name>

Arguments

name Name of the compression action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the action is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cmp action" or 'my cmp action').

cmpType Type of compression performed by this action. Available settings function as follows:

- COMPRESS - Apply GZIP or DEFLATE compression to the response, depending on the request header. Prefer GZIP.
- GZIP - Apply GZIP compression.
- DEFLATE - Apply DEFLATE compression.
- NOCOMPRESS - Do not compress the response if the request matches a policy that uses this action.

Possible values: compress, gzip, deflate, nocompress

addVaryHeader Control insertion of the Vary header in HTTP responses compressed by Citrix ADC. Intermediate caches store different versions of the response for different values of the headers present in the Vary response header.

Possible values: GLOBAL, DISABLED, ENABLED Default value: GLOBAL

varyHeaderValue The value of the HTTP Vary header for compressed responses.
   ```

Example

set cmp action cmpact1 -addVaryHeader ENABLED -varyHeaderValue User-Agent

add cmp action

Creates a compression action. Note: User-defined compression actions supplement the built-in compression actions. The built-in compression actions, NOCOMPRESS, COMPRESS, GZIP, and DEFLATE, are always available. Available settings functions as follows:

- NOCOMPRESS - Disables compression for data that matches the associated policy.
- COMPRESS - Enable GZIP or DEFLATE compression, depending on which is supported by the browser.
- GZIP - Enable GZIP compression. For browsers that do not support GZIP, compression is disabled.
- DEFLATE - Enable DEFLATE compression for a specific policy. For browsers that do not support DEFLATE, compression is disabled.

Synopsis

add cmp action <name> <cmpType>

Arguments

name Name of the compression action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the action is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cmp action" or 'my cmp action').

cmpType Type of compression performed by this action. Available settings function as follows:

- COMPRESS - Apply GZIP or DEFLATE compression to the response, depending on the request header. Prefer GZIP.
- GZIP - Apply GZIP compression.
- DEFLATE - Apply DEFLATE compression.
- NOCOMPRESS - Do not compress the response if the request matches a policy that uses this action.

Possible values: compress, gzip, deflate, nocompress

addVaryHeader Control insertion of the Vary header in HTTP responses compressed by Citrix ADC. Intermediate caches store different versions of the response for different values of the headers present in the Vary response header.

Possible values: GLOBAL, DISABLED, ENABLED Default value: GLOBAL

varyHeaderValue The value of the HTTP Vary header for compressed responses.

Example

add cmp action nocmp NOCOMPRESS

rm cmp action

Removes the specified compression action.

Synopsis

rm cmp action <name>

Arguments

name Name of the action to be removed.

Example

rm cmp action cmp_action_name

Cmp

The entities on which you can perform NetScaler CLI operations:

- cmp-action
- cmp
- cmp-global
- cmp-parameter
- cmp-policy
- cmp-policylabel
- cmp-stats

cmp-global

The following operations can be performed on "cmp-global":

bind| show| unbind|

bind cmp global

Binds (activates) the compression policy globally. Note that the compression feature requires a compression license. When you enable the compression feature, all of the built-in compression policies are bound globally.

Synopsis

bind cmp global <policyName>

Arguments

policyName Name of the policy to bind globally.

priority Positive integer specifying the priority of the policy. The lower the number, the higher the priority. By default, polices within a label are evaluated in the order of their priority numbers. In the configuration utility, you can click the Priority field and edit the priority level or drag the entry to a new position in the list. If you drag the entry to a new position, the priority level is updated automatically. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the priority of the next policy, within the policy label, to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher numbered priority.
- END - Stop evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, it's evaluation result determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, that policy is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher priority number is evaluated next.

- If the expression evaluates to a priority number that is numerically higher than the highest priority number, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

type Global bind point, specifying where to bind the policy.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, HTTPQUIC_RES_OVERRIDE, HTTPQUIC_RES_DEFAULT, NONE Default value: NONE

invoke Invoke policies bound to a virtual server or a policy label. After the invoked policies are evaluated, the flow returns to the policy with the next priority.

labelType Type of policy label invocation.

Possible values: reqvserver, resvserver, policylabel

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

Example

add cmp policy pdf_cmp -rule "HTTP.RES.HEADER(\"Content-Type\").CONTAINS(\"application/pdf\")" -resAction COMPRESS

After creating the above compression policy, you must activate it by binding it globally: bind cmp global pdf_cmp -priority 100

After binding pdf_cmp compression policy globally, the policy gets activated and the Citrix ADC system will perform compression for the pdf files

show cmp global

Displays the globally bound HTTP compression policies.

Synopsis

show cmp global

Arguments

type Bind point to which the policy is bound.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, HTTPQUIC_RES_OVERRIDE, HTTPQUIC_RES_DEFAULT, NONE

Output

stateflag policyName The name of the globally bound HTTP compression policy.

priority Positive integer specifying the priority of the policy. The lower the number, the higher the priority. By default, polices within a label are evaluated in the order of their priority numbers. In the configuration utility, you can click the Priority field and edit the priority level or drag the entry to a new position in the list. If you drag the entry to a new position, the priority level is updated automatically.

numpol The number of policies bound to the bindpoint.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE

invoke Invoke flag.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

globalBindType devno count

Example

> show cmp global Global bindpoint: RES_DEFAULT Number of bound policies: 5 Done

unbind cmp global

Deactivates a globally bound HTTP compression policy.

Synopsis

unbind cmp global <policyName> [-type <type>]

Arguments

policyName Name of the compression policy to unbind.

type Bind point, specifying from where to unbind the policy.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, HTTPQUIC_RES_OVERRIDE, HTTPQUIC_RES_DEFAULT, NONE

priority Integer specifying the priority of the policy. The lower the number, the higher the priority. By default, polices within a label are evaluated in the order of their priority numbers. Note that in the configuration utility, you can click the Priority field and edit the priority level or drag the entry to a new position in the list. If you drag the entry to a new position, the priority level is updated automatically. Minimum value: 1 Maximum value: 2147483647

Example

unbind cmp global pdf_cmp

cmp-parameter

The following operations can be performed on "cmp-parameter":

show| unset| set|

show cmp parameter

Displays the values of the compression parameters. Example: > show cmp parameter Configured compression parameters: Compression level: optimal Quantum size: 4555 Server-side compression: ON Minimum HTTP response size for compression: 0 CPU load at which to bypass compression: 100% Compression on PUSH: DISABLED Vary header insertion: DISABLED Disable external cache: NO

Synopsis

show cmp parameter

Arguments

Output

cmpLevel Specify a compression level. Available settings function as follows:

- Optimal - Corresponds to a gzip GZIP level of 5-7.
- Best speed - Corresponds to a gzip level of 1.
- Best compression - Corresponds to a gzip level of 9.

quantumSize Minimum quantum of data to be filled before compression begins.

serverCmp Compression enabled/disabled at back-end server.

heurExpiry Heuristic basefile expiry.

heurExpiryThres Threshold compression ratio for heuristic basefile expiry, multiplied by 100. For example, to set the threshold ratio to 1.25, specify 125.

heurExpiryHistWt For heuristic basefile expiry, weightage to be given to historical delta compression ratio, specified as percentage. For example, to give 25% weightage to historical ratio (and therefore 75% weightage to the ratio for current delta compression transaction), specify 25.

minResSize Smallest response size, in bytes, to be compressed.

cmpBypassPct Citrix ADC CPU threshold after which compression is not performed. Range: 0 - 100

cmpOnPush Citrix ADC does not wait for the quantum to be filled before starting to compress data. Upon receipt of a packet with a PUSH flag, the appliance immediately begins compression of the accumulated packets.

policyType Type of the policy. The only possible value is ADVANCED

addVaryHeader Control insertion of the Vary header in HTTP responses compressed by Citrix ADC. Intermediate caches store different versions of the response for different values of the headers present in the Vary response header.

varyHeaderValue The value of the HTTP Vary header for compressed responses. If this argument is not specified, a default value of "Accept-Encoding" will be used.

externalCache Enable insertion of Cache-Control: private response directive to indicate response message is intended for a single user and must not be cached by a shared or proxy cache.

builtin Flag to determine whether compression is default or not

feature The feature to be checked while applying this config

unset cmp parameter

Reverts to the default value.Refer to the set cmp parameter command for meanings of the arguments.

Synopsis

unset cmp parameter

Example

unset cmp param -policytype

set cmp parameter

Configures the compression parameters.

Synopsis

set cmp parameter [-addVaryHeader (ENABLED | DISABLED)]

Arguments

cmpLevel Specify a compression level. Available settings function as follows:

- Optimal - Corresponds to a gzip GZIP level of 5-7.
- Best speed - Corresponds to a gzip level of 1.
- Best compression - Corresponds to a gzip level of 9.

Possible values: optimal, bestspeed, bestcompression Default value: optimal

quantumSize Minimum quantum of data to be filled before compression begins. Default value: 57344 Minimum value: 8 Maximum value: 63488

serverCmp Allow the server to send compressed data to the Citrix ADC. With the default setting, the Citrix ADC appliance handles all compression.

Possible values: ON, OFF Default value: ON

minResSize Smallest response size, in bytes, to be compressed. Minimum value: 0

cmpBypassPct Citrix ADC CPU threshold after which compression is not performed. Range: 0 - 100 Default value: 100 Minimum value: 0 Maximum value: 100

cmpOnPush Citrix ADC does not wait for the quantum to be filled before starting to compress data. Upon receipt of a packet with a PUSH flag, the appliance immediately begins compression of the accumulated packets.

Possible values: ENABLED, DISABLED Default value: DISABLED

policyType Type of the policy. The only possible value is ADVANCED

Possible values: ADVANCED Default value: ADVANCED

addVaryHeader Control insertion of the Vary header in HTTP responses compressed by Citrix ADC. Intermediate caches store different versions of the response for different values of the headers present in the Vary response header.

Possible values: ENABLED, DISABLED Default value: DISABLED

varyHeaderValue The value of the HTTP Vary header for compressed responses. If this argument is not specified, a default value of "Accept-Encoding" will be used.

externalCache Enable insertion of Cache-Control: private response directive to indicate response message is intended for a single user and must not be cached by a shared or proxy cache.

Possible values: YES, NO Default value: NO

Example

set cmp param -cmpLevel bestspeed -quantumSize 20480

cmp-policy

The following operations can be performed on "cmp-policy":

add| show| rename| stat| rm| set|

add cmp policy

Creates a HTTP compression policy. When the policy matches an HTTP request or response, the action specified in the policy is performed on the transaction. The policy can be bound globally or to an entity. For the policy to have an effect, compression must be enabled on the service.

Synopsis

add cmp policy <name> -rule <expression> -resAction <string>

Arguments

name Name of the HTTP compression policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cmp policy" or 'my cmp policy').

rule Expression that determines which HTTP requests or responses match the compression policy.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

resAction The built-in or user-defined compression action to apply to the response when the policy matches a request or response.

Example

Example 1:

add cmp policy pdf_cmp -rule "HTTP.RES.HEADER(\"Content-Type\").CONTAINS(\"application/pdf\")" -resAction COMPRESS

After creating the above compression policy, you must activate it by binding it globally: bind cmp global pdf_cmp -priority 100

The Citrix ADC system will use the configured pdf_cmp compression policy to perform compression of pdf files.

Example 2:

The following command disables compression for all the access from the specific subnet. add cmp policy local_sub_nocmp -rule "CLIENT.IP.SRC.IN_SUBNET(10.1.1.0/24)" -resAction NOCOMPRESS bind cmp global local_sub_nocmp -priority 200

show cmp policy

Displays details of all HTTP compression policies.

Synopsis

show cmp policy show cmp policy stats - alias for 'stat cmp policy'

Arguments

name Name of the HTTP compression policy for which to display details.

Output

stateflag rule The request/response rule that will trigger the specified compression action.

reqAction The compression action to be performed on requests.

resAction The compression action to be performed on responses.

hits Number of hits.

txbytes Number of bytes transferred.

rxbytes Number of bytes received.

clientTTLB Total client TTLB value.

clientTransactions Number of client transactions.

serverTTLB Total server TTLB value.

serverTransactions Number of server transactions.

boundTo The name of the entity to which the policy is bound.

activePolicy priority gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

description Description of the policy

vserverType builtin Flag to determine if compression policy is builtin or not

feature The feature to be checked while applying this config

type isDefault A value of true is returned if it is a default policy

devno count

Example

show cmp policy 4 Compression policies:

1. ```
   Name: ns_adv_cmp_content_type       Rule: HTTP.RES.HEADER("Content-
   Type").CONTAINS("text")

   Response action: COMPRESS       Hits: 1

   Bytes In:...4325        Bytes Out:... 1530

   Bandwidth saving...64.62%       Ratio 2.83:1
   ```

2. ```
   Name: ns_adv_cmp_mscss      Rule: (ns_msie_adv &&
   HTTP.RES.HEADER("Content-Type").CONTAINS("text/css"))

   Response action: COMPRESS       Hits: 0
   ```

3. ```
   Name: ns_adv_nocmp_mozilla_47       Rule: (HTTP.REQ.HEADER("User-
   Agent").CONTAINS("Mozilla/4.7") && HTTP.RES.HEADER("Content-
   Type").CONTAINS("text/css"))

   Response action: NOCOMPRESS     Hits: 0
   ```

Done

You can also view an individual cmp policy by giving the cmp policy name as an argument:

show cmp policy ns_adv_cmp_content_type Name: ns_adv_cmp_content_type Rule: HTTP.RES.HEADER("Content-Type").CONTAINS("text") Response action: COMPRESS Hits: 7 Bytes In:...796160 Bytes Out:... 197730 Bandwidth saving...75.16% Ratio 4.03:1 Done
   ```

rename cmp policy

Renames a compression policy.

Synopsis

rename cmp policy <name>@ <newName>@

Arguments

name Existing name of the policy.

newName New name for the compression policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Choose a name that reflects the function that the policy performs.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cmp policy" or 'my cmp policy').

Example

rename cmp policy oldname newname

stat cmp policy

Displays compression statistics for all compression policies, or for only the specified policy.

Synopsis

stat cmp policy

Arguments

name Name of the compression policy for which to display statistics. If no name is specified, statistics for all compression polices are shown.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Policy undef hits (Undefhits) Number of undef hits on the policy

Example

stat cmp policy

Related Commands

- stat cmp policylabel

rm cmp policy

Removes a user-defined HTTP compression policy.

Synopsis

rm cmp policy <name>

Arguments

name Name of the HTTP compression policy to be removed.

Example

rm cmp policy cmp_policy_name The "show cmp policy" command shows all currently defined HTTP compression policies.

set cmp policy

Modifies the specified parameters of an HTTP compression policy. Note: Use the show cmp policy command to view all configured HTTP compression policies.

Synopsis

set cmp policy <name>

Arguments

name Name of the HTTP compression policy to be modified.

rule New rule to be associated with the HTTP compression policy. You can modify the existing rule or create a new rule.

resAction The built-in or user-defined compression action to be associated with the policy.

Example

Example 1:

add cmp policy pdf_cmp -rule "HTTP.RES.HEADER(\"Content-Type\").CONTAINS(\"application/pdf\")" -resAction COMPRESS

After creating the above compression policy, you must activate it by binding it globally: bind cmp global pdf_cmp -priority 100

The Citrix ADC system will use the configured pdf_cmp compression policy to perform compression for pdf files.

To disable pdf compression for Internet Explorer, you can change the above compression policy by issuing the following command:

set cmp policy pdf_cmp -rule "HTTP.RES.HEADER(\"Content-Type\").CONTAINS(\"application/pdf\") && HTTP.RES.HEADER(\"User-Agent\").CONTAINS(\"MSIE\").NOT"

To view the changed cmp policy, enter the following command:

> show cmp policy pdf_cmp Name: pdf_cmp Rule: ("HTTP.RES.HEADER(\"Content-Type\").CONTAINS(\"application/pdf\") && HTTP.RES.HEADER(\"User-Agent\").CONTAINS(\"MSIE\").NOT) Response action: COMPRESS Hits: 2 Bytes In:...609284 Bytes Out:... 443998 Bandwidth saving...27.13% Ratio 1.37:1 Done

cmp-policylabel

The following operations can be performed on "cmp-policylabel":

unbind| show| add| rename| bind| stat| rm|

unbind cmp policylabel

Unbinds an HTTP compression policy from an HTTP compression policy label.

Synopsis

unbind cmp policylabel <labelName> <policyName>

Arguments

labelName Name of the HTTP compression policy label from which to unbind the policy.

policyName Name of the HTTP compression policy to unbind from the policy label.

priority Priority of the NOPOLICY to unbind. Required only to unbind a NOPOLICY, if it has been bound to this policy label. Minimum value: 1 Maximum value: 2147483647

Example

unbind cmp policylabel cmp_pol_label cmp_pol

show cmp policylabel

Displays details of configured HTTP compression policy labels.

Synopsis

show cmp policylabel

Arguments

labelName Name of the HTTP compression policy label for which to display details.

Output

stateflag type Type of packets (request packets or response) against which to match the policies bound to this policy label.

numpol Number of polices bound to label.

hits Number of times policy label was invoked.

policyName The compression policy name.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke Invoke policies bound to a virtual server or a user-defined policy label. After the invoked policies are evaluated, the flow returns to the policy with the next higher priority number in the original label.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy evaluates to TRUE.

flowType Flowtype of the bound compression policy.

description Description of the policylabel

flags devno count

Example

i)show cmp policylabel cmp_pol_label ii)show cmp policylabel

add cmp policylabel

Creates a user-defined HTTP compression policy label. Policies that you bind to the label are evaluated only if you call the label from another policy.

Synopsis

add cmp policylabel <labelName> -type <type>

Arguments

labelName Name of the HTTP compression policy label. Must begin with a letter, number, or the underscore character (_). Additional characters allowed, after the first character, are the hyphen (-), period (.) pound sign (#), space ( ), at sign (@), equals (=), and colon (:). The name must be unique within the list of policy labels for compression policies. Can be renamed after the policy label is created.

> The following requirement applies only to the Citrix ADC CLI:

If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cmp policylabel" or 'my cmp policylabel').

type Type of packets (request packets or response) against which to match the policies bound to this policy label.

Possible values: REQ, RES, HTTPQUIC_REQ, HTTPQUIC_RES

Example

add cmp policylabel cmp_pol_label -type REQ

rename cmp policylabel

Renames a compression policylabel.

Synopsis

rename cmp policylabel <labelName>@ <newName>@

Arguments

labelName Existing name of the policy label.

newName New name for the compression policy label. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

> `The following requirement applies only to the Citrix ADC CLI:`

If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cmp policylabel" or 'my cmp policylabel').

Example

rename cmp policylabel oldname newname

bind cmp policylabel

Binds an HTTP compression policy to an HTTP compression policy label.

Synopsis

bind cmp policylabel <labelName> -policyName <string> -priority <positive_integer>

Arguments

labelName Name of the HTTP compression policy label to which to bind the policy.

policyName Name of the compression policy to bind to the label.

priority Integer specifying the priority of the policy. The lower the number, the higher the priority. By default, polices within a label are evaluated in the order of their priority numbers. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the priority of the next policy, within the policy label, to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher numbered priority.
- END - Stop evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, it's evaluation result determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, that policy is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher priority number is evaluated next.
- If the expression evaluates to a priority number that is numerically higher than the highest priority number, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

invoke Invoke policies bound to a virtual server or a user-defined policy label. After the invoked policies are evaluated, the flow returns to the policy with the next higher priority number in the original label.

labelType Type of policy label invocation.

Possible values: reqvserver, resvserver, policylabel

labelName Name of the label to invoke if the current policy evaluates to TRUE.

Example

bind cmp policylabel cmp_pol_label -policyName cmp_pol -priority 100

stat cmp policylabel

Displays statistics for all compression policy labels.

Synopsis

stat cmp policylabel

Arguments

labelName Name of the compression policy label for which to display statistics. If not specified, statistics are displayed for all compression policy labels.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy Label Hits (Hits) Number of times policy label was invoked.

rm cmp policylabel

Removes an HTTP compression policy label.

Synopsis

rm cmp policylabel <labelName>

Arguments

labelName Name of the HTTP compression policy label to be removed.

Example

rm cmp policylabel cmp_pol_label

cmp-stats

The following operations can be performed on "cmp-stats":

show cmp stats

show cmp stats is an alias for stat cmp Displays compression statistics.

Synopsis

show cmp stats - alias for 'stat cmp'

cmp

The following operations can be performed on "cmp":

stat cmp

Display compression statistics.

Synopsis

stat cmp

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Bandwidth saving (%) (DlBndSav) Bandwidth saving from delta compression expressed as percentage.

Delta compression ratio (DlCmpRt) Ratio of compressible data received to compressed data transmitted.If this ratio is one (uncmp:1.0) that means compression is disabled or we are not able to compress even a single compressible packet.

Decompression ratio (DTCmpRt) Ratio of decompressed data transmitted to compressed data received.

Bandwidth saving (%) (DBndSav) Bandwidth saving from TCP compression expressed as percentage.

TCP compression ratio (TCmpRt) Ratio of compressible data received to compressed data transmitted.If this ratio is one (uncmp:1.0) that means compression is disabled or we are not able to compress even a single compressible packet.

TCP Bandwidth saving (%) (BndSav) Bandwidth saving from TCP compression expressed as percentage.

Total HTTP compression ratio Ratio of total HTTP data received to total HTTP data transmitted.

HTTP Bandwidth saving (%) (HttpBndSav) Bandwidth saving from TCP compression expressed as percentage.

HTTP compression ratio Ratio of the compressible data received from the server to the compressed data sent to the client.

HTTP compression requests Number of HTTP compression requests the Citrix ADC receives for which the response is successfully compressed. For example, after you enable compression and configure services, if you send HTTP requests to the Citrix ADC using a HTTP client that supports

compression, and Citrix ADC compresses the corresponding response, this counter is incremented.

Compressible bytes received Number of bytes that can be compressed, which the Citrix ADC receives from the server. This gives the content length of the response that the Citrix ADC receives from server.

Compressed bytes transmitted Number of bytes the Citrix ADC sends to the client after compressing the response from the server.

Compressible packets received Number of HTTP packets that can be compressed, which the Citrix ADC receives from the server.

Compressed packets transmitted Number of HTTP packets that the Citrix ADC sends to the client after compressing the response from the server.

Compressible bytes received (TCmpRxB) Number of bytes that can be compressed, which the Citrix ADC receives from the server. This gives the content length of the response that the Citrix ADC receives from server.

Compressible packets received (TCmpRxP) Total number of compressible packets received by Citrix ADC.

Compressed bytes transmitted (TCmpTxB) Number of bytes that the Citrix ADC sends to the client after compressing the response from the server.

Compressed packets transmitted (TCmpTxP) Number of TCP packets that the Citrix ADC sends to the client after compressing the response from the server.

Quantum compression (TCmpQuan) Number of times the Citrix ADC compresses a quantum of data. Citrix ADC buffers the data received from the server till it reaches the quantum size and then compresses the buffered data and transmits to the client.

Push flag compression (TCmpPush) Number of times the Citrix ADC compresses data on receiving a TCP PUSH flag from the server. The PUSH flag ensures that data is compressed immediately without waiting for the buffered data size to reach the quantum size.

End Of Input compression (TCmpEoi) Number of times the Citrix ADC compresses data on receiving End Of Input (FIN packet). When the Citrix ADC receives End Of Input (FIN packet), it compresses the buffered data immediately without waiting for the buffered data size to reach the quantum size.

Timer compression (TCmpTmr) Number of times the Citrix ADC compresses data on expiration of data accumulation timer. The timer expires if the server response is very slow and consequently, the Citrix ADC does not receive response for a certain amount of time. Under such a condition, the Citrix ADC compresses the buffered data immediately without waiting for the buffered data size to reach the quantum size.

Compressed bytes received (DCmpTRxB) Total number of compressed bytes received by Citrix ADC.

Compressed packets received (DCmpTRxP) Total number of compressed packets received by Citrix ADC.

Decompressed bytes transmitted (DCmpTTxB) Total number of decompressed bytes transmitted by Citrix ADC.

Decompressed packets transmitted (DCmpTTxP) Total number of decompressed packets transmitted by Citrix ADC.

Wrong data (DCmpErrD) Number of data errors encountered while decompressing.

Less Data (DCmpErrL) Number of times Citrix ADC received less data than declared by protocol.

More Data (DCmpErrM) Number of times Citrix ADC received more data than declared by protocol.

Memory failures (DCmpMem) Number of times memory failures occurred while decompressing.

Unknown (DCmpErrU) Number of times unknown errors occurred while decompressing.

Delta compression requests (DlCmpRx) Total number of delta compression requests received by Citrix ADC.

Delta compression applied (DlDone) Total number of delta compressions done by Citrix ADC.

Compressible bytes received (DlCmpRxB) Total number of delta-compressible bytes received by Citrix ADC.

Compressed bytes transmitted (DlCmpTxB) Total number of delta-compressed bytes transmitted by Citrix ADC.

First-time access (DlCmpFAc) Total number of delta compression first accesses.

Compressible packets received (DlCmpRxP) Number of delta-compressible packets received.

Compressed packets transmitted (DlCmpTxP) Total number of delta-compressed packets transmitted by Citrix ADC.

Basefile requests served (DlCBSrv) Total number of basefile requests served by Citrix ADC.

Basefile bytes transmitted (DlCBTxB) Number of basefile bytes transmitted by Citrix ADC.

Delta compression bypassed (DlCmpEBy) Number of times delta-compression bypassed by Citrix ADC.

Basefile write header failed (DlCmpEBW) Number of times basefile could not be updated in Citrix ADC cache.

Basefile no-store miss (DlCmpENM) Number of times basefile was not found in Citrix ADC cache.

Request information too big (DlCmpERB) Number of times basefile request URL was too large.

Request info alloc failed (DlCmpERF) Number of times requested basefile could not be allocated.

Session allocation failed (DlCmpESF) Number of times delta compression session could not be allocated.

Response bytes received (HTRspbRx) Total number of bytes of HTTP response data received.

Related Commands

- stat cmp policylabel

contentinspection

contentinspection-action

The following operations can be performed on "contentinspection-action":

show| unset| add| set| rm|

show contentinspection action

Displays information about a RemoteService action. If no name is specified, this command displays information of all available RemoteService actions.

Synopsis

show contentinspection action

Arguments

name Name of the RemoteService action.

Output

type Type of RemoteService action.

serverName Lb vserver or service name.

serverip IP address of remoteService

serverport Port of remoteService

icapProfileName Name of the ICAP profile to be attached to the contentInspection action.

ifserverdown Name of the action to perform if the Vserver representing the remote service is not UP. This is not supported for NOINSPECTION Type. The Supported actions are:

- RESET - Reset the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend the request if desired.
- DROP - Drop the request without sending a response to the user.

- CONTINUE - It bypasses the ContentIsnpection and Continues/resumes the Traffic-Flow to Client/Server.

reqTimeout Time, in seconds, within which the remote service request must complete. This is not supported for NOINSPECTION action type. If the request does not complete within this time, the specified request timeout action is executed. Zero disables the timeout.

reqTimeoutAction Name of the action to perform if the Vserver representing the remote service does not respond. This is not supported for NOINSPECTION action type. There are also some built-in actions which can be used. These are:

- RESET - Reset the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend the request if desired.
- DROP - Drop the request without sending a response to the user.

hits The number of times the action has been taken.

referenceCount The number of references to the action.

undefHits The number of times the action resulted in UNDEF.

stateflag builtin Flag to determine whether contentinspection action is built-in or not

feature The feature to be checked while applying this config

devno count

Example

1. show contentinspection action
2. show contentinspection action act_icap

unset contentinspection action

Use this command to remove contentinspection action settings.Refer to the set contentinspection action command for meanings of the arguments.

Synopsis

unset contentinspection action <name>

add contentinspection action

Creates a RemoteService action.

Synopsis

add contentinspection action <name> -type <type> (-serverName <string> | (-serverip <ip_addr|ipv6_addr>))

Arguments

name Name of the remote service action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

type Type of operation this action is going to perform. following actions are available to configure:

- ICAP - forward the incoming request or response to an ICAP server for modification.
- INLINEINSPECTION - forward the incoming or outgoing packets to IPS server for Intrusion Prevention.
- MIRROR - Forwards cloned packets for Intrusion Detection.
- NOINSPECTION - This does not forward incoming and outgoing packets to the Inspection device.
- NSTRACE - capture current and further incoming packets on this transaction.

Possible values: ICAP, INLINEINSPECTION, MIRROR, NOINSPECTION

serverName Name of the LB vserver or service

serverip IP address of remoteService

serverport Port of remoteService Default value: 1344 Minimum value: 1 Maximum value: 65535

icapProfileName Name of the ICAP profile to be attached to the contentInspection action.

ifserverdown Name of the action to perform if the Vserver representing the remote service is not UP. This is not supported for NOINSPECTION Type. The Supported actions are:

- RESET - Reset the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend the request if desired.
- DROP - Drop the request without sending a response to the user.
- CONTINUE - It bypasses the ContentIsnpection and Continues/resumes the Traffic-Flow to Client/Server.

Possible values: CONTINUE, DROP, RESET Default value: RESET

set contentinspection action

Modifies the specified parameters of a RemoteService action.

Synopsis

set contentinspection action <name>

Arguments

name Name of the RemoteService policy to modify.

serverName Name of the LB vserver or service

serverip IP address of remoteService

serverport Port of remoteService Default value: 1344 Minimum value: 1 Maximum value: 65535

icapProfileName Name of the ICAP profile to be attached to the contentInspection action.

ifserverdown Name of the action to perform if the Vserver representing the remote service is not UP. This is not supported for NOINSPECTION Type. The Supported actions are:

- RESET - Reset the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend the request if desired.
- DROP - Drop the request without sending a response to the user.
- CONTINUE - It bypasses the ContentIsnpection and Continues/resumes the Traffic-Flow to Client/Server.

Possible values: CONTINUE, DROP, RESET Default value: RESET

Example

set contentinspection action caact1 -type IPS"

rm contentinspection action

Removes a contentinspection action.

Synopsis

rm contentinspection action <name>

Arguments

name Name of the RemoteService action to remove.

Example

rm contentinspection action act_before

contentinspection-callout

The following operations can be performed on "contentinspection-callout":

add| show| rm| set| unset|

add contentinspection callout

Adds an expression element that, when evaluated, sends a request to Content Inspection service and receives a response from the service. Can be used to obtain additional information for use in evaluating policy rules and other expressions. The expression prefix SYS.CI_CALLOUT invokes a Content Inspection callout.

Synopsis

add contentinspection callout <name> -type ICAP (-serverName <string> | (-serverip <ip_addr|ipv6_addr>)) -returnType <returnType> -resultExpr <string>

Arguments

name Name for the Content Inspection callout. Not case sensitive. Must begin with an ASCII letter or underscore (_) character, and must consist only of ASCII alphanumeric or underscore characters. Must not begin with 're' or 'xp' or be a word reserved for use as an expression qualifier prefix (such as HTTP) or enumeration value (such as ASCII). Must not be the name of an existing named expression, pattern set, dataset, stringmap, or callout.

type Type of the Content Inspection callout. It must be one of the following:

- ICAP - Sends ICAP request to the configured ICAP server.

Possible values: ICAP

profileName Name of the Content Inspection profile. The type of the configured profile must match the type specified using -type argument.

serverName Name of the load balancing or content switching virtual server or service to which the Content Inspection request is issued. Mutually exclusive with server IP address and port parameters. The service type must be TCP or SSL_TCP. If there are vservers and services with the same name, then vserver is selected.

serverip IP address of Content Inspection server. Mutually exclusive with the server name parameter.

serverport Port of the Content Inspection server. Default value: 1344 Minimum value: 1 Maximum value: 65535

returnType Type of data that the target callout agent returns in response to the callout. Available settings function as follows:

- TEXT - Treat the returned value as a text string.
- NUM - Treat the returned value as a number.
- BOOL - Treat the returned value as a Boolean value. Note: You cannot change the return type after it is set.

Possible values: BOOL, NUM, TEXT

resultExpr Expression that extracts the callout results from the response sent by the CI callout agent. Must be a response based expression, that is, it must begin with ICAP.RES. The operations in this expression must match the return type. For example, if you configure a return type of TEXT, the result expression must be a text based expression, as in the following example: icap.res.header("ISTag")

comment Any comments to preserve information about this Content Inspection callout.

Example

add contentInspection callout cic

show contentinspection callout

Displays information about the configured Content Inspection callouts.

Synopsis

show contentinspection callout

Arguments

name Name of the Content Inspection callout to display. If a name is not provided, information about all configured Content Inspection callouts is shown.

Output

stateflag type Type

profileName Profile name

serverName Vserver/Server name

serverip Server IP address.

serverport Server port.

returnType Return type of the callout

resultExpr String expression for callout response

hits Total hits

undefHits Total undefs

undefReason Reason for last undef

comment Any comments to preserve information about this Content Inspection callout.

devno count

Example

show contentInspection callout cic

rm contentinspection callout

Removes a Content Inspection callout. You cannot remove a Content Inspection callout that is used in any part of policy, action, or expression.

Synopsis

rm contentinspection callout <name>

Arguments

name Name of the Content Inspection callout to remove.

Example

rm contentInspection callout cic

set contentinspection callout

Modifies the attributes of an existing Content Inspection callout element.

Synopsis

set contentinspection callout <name>

Arguments

name Name of the Content Inspection callout to configure.

serverName Name of the load balancing or content switching virtual server or service to which the Content Inspection request is issued. Mutually exclusive with server IP address and port parameters. The service type must be TCP or SSL_TCP. If there are vservers and services with the same name, then vserver is selected.

serverip IP address of Content Inspection server. Mutually exclusive with the server name parameter.

serverport Port of the Content Inspection server. Default value: 1344 Minimum value: 1 Maximum value: 65535

profileName Name of the Content Inspection profile. The type of the configured profile must match the type specified using -type argument.

returnType Type of data that the target callout agent returns in response to the callout. Available settings function as follows:

- TEXT - Treat the returned value as a text string.
- NUM - Treat the returned value as a number.
- BOOL - Treat the returned value as a Boolean value. Note: You cannot change the return type after it is set.

Possible values: BOOL, NUM, TEXT

resultExpr Expression that extracts the callout results from the response sent by the CI callout agent. Must be a response based expression, that is, it must begin with ICAP.RES. The operations in this expression must match the return type. For example, if you configure a return type of TEXT, the result expression must be a text based expression, as in the following example: icap.res.header("ISTag")

comment Any comments to preserve information about this Content Inspection callout.

Example

set contentInspection callout cic -profileName NewProfileName

unset contentinspection callout

Use this command to remove contentinspection callout settings.Refer to the set contentinspection callout command for meanings of the arguments.

Synopsis

unset contentinspection callout <name>

contentinspection-global

The following operations can be performed on "contentinspection-global":

unbind| bind| show|

unbind contentinspection global

Unbinds the specified contentInspection policy from contentInspection global. See the bind contentInspection global command for a description of the parameters.

Synopsis

unbind contentinspection global -policyName <string>

Arguments

policyName Name of the contentInspection policy to deactivate.

type The bindpoint from which to unbind.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

priority Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind contentInspection global pol9

bind contentinspection global

Activates the specified contentInspection policy globally.

Synopsis

bind contentinspection global -policyName <string> -priority <positive_integer>

Arguments

policyName Name of the contentInspection policy to activate.

priority Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Must be unique within the label. Policies are evaluated in the order of their priorities, and the first policy that matches the request or response is applied. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.
- The expression evaluates to a priority number that is smaller than the current policyÂ’s priority number.
- The expression evaluates to a priority number that is between the current policyÂ’s priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

type Bind point to which to bind the policy. Available settings function as follows:

- REQ_OVERRIDE - Request override. Binds the policy to the priority request queue.
- REQ_DEFAULT - Binds the policy to the default request queue.
- RES_OVERRIDE - Response override. Binds the policy to the priority response queue. RES_DEFAULT - Binds the policy to the default response queue.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

invoke Terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

labelType Type of invocation. Available settings function as follows:

- reqvserver - Forward the request to the specified request virtual server.
- resvserver - Forward the response to the specified response virtual server.
- policylabel - Invoke the specified policy label.

Possible values: reqvserver, resvserver, policylabel

labelName

- If labelType is policylabel, name of the policy label to invoke.
- If labelType is reqvserver or resvserver, name of the virtual server to which to forward the request of response.

Example

i)bind contentInspection global -policyName pol9 -priority 9 ii)bind contentInspection global -policyName pol9 -priority 9 -gotoPriorityExpression 120 iii)bind contentInspection global pol9 9 -gotoPriorityExpression "HTTP.REQ.HEADER(\\"qh3\\").TYPECAST_NUM_T(DECIMAL)"

show contentinspection global

Displays the list of policies bound to the specified contentInspection global policy bank. If no policy bank is specified, displays a list of all policies bound to contentInspection global.

Synopsis

show contentinspection global

Arguments

type The bindpoint to which to policy is bound.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

Output

stateflag policyName Name of the contentInspection policy.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke Terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

labelType Type of invocation. Available settings function as follows:

- reqvserver - Forward the request to the specified request virtual server.
- resvserver - Forward the response to the specified response virtual server.
- policylabel - Invoke the specified policy label.

labelName

- If labelType is policylabel, name of the policy label to invoke.
- If labelType is reqvserver or resvserver, name of the virtual server to which to forward the request of response.

numpol The number of policies bound to the bindpoint.

flowType flowtype of the bound contentInspection policy.

flags globalBindType devno count

Example

show contentInspection global

contentinspection-parameter

The following operations can be performed on "contentinspection-parameter":

set| unset| show|

set contentinspection parameter

Sets the given contentisnpection parameter(s).

Synopsis

set contentinspection parameter -undefAction <string>

Arguments

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an error condition in evaluating the expression. Available settings function as follows:

- NOINSPECTION - Do not Inspect the traffic.
- RESET - Reset the connection and notify the user's browser, so that the user can resend the request.
- DROP - Drop the message without sending a response to the user. Default value: "NOINSPECTION"

Example

set contentinspection parameter -undefAction RESET

unset contentinspection parameter

Resets the given CI parameter(s)..Refer to the set contentinspection parameter command for meanings of the arguments.

Synopsis

unset contentinspection parameter -undefAction

Example

unset contentinspection parameter -undefAction

show contentinspection parameter

Displays the Contentinspection parameters.

Synopsis

show contentinspection parameter

Arguments

Output

undefAction Name of the contentinspection undef action.

timeout Timeout.

Example

show contentinspection parameter

contentinspection-policy

The following operations can be performed on "contentinspection-policy":

rename| add| set| stat| rm| unset| show|

rename contentinspection policy

Renames the specified contentInspection policy.

Synopsis

rename contentinspection policy <name>@ <newName>@

Arguments

name Existing name of the contentInspection policy.

newName New name for the contentInspection policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my contentInspection policy" or 'my contentInspection policy').

Example

rename contentInspection policy oldname newname

add contentinspection policy

Creates a contentInspection policy, which specifies requests that the Citrix ADC intercepts and executes the specified action.

Synopsis

add contentinspection policy <name> -rule <expression> -action <string>

Arguments

name Name for the contentInspection policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the contentInspection policy is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my contentInspection policy" or 'my contentInspection policy').

rule Expression that the policy uses to determine whether to execute the specified action.

action Name of the contentInspection action to perform if the request matches this contentInspection policy. There are also some built-in actions which can be used. These are:

- NOINSPECTION - Send the request from the client to the server or response from the server to the client without sending it to Inspection device for Content Inspection.
- RESET - Resets the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend the request if desired.
- DROP - Drop the request without sending a response to the user.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

comment Any type of information about this contentInspection policy.

logAction Name of the messagelog action to use for requests that match this policy.

Example

i) add contentInspection policy pol9 -rule "HTTP.REQ.URL.URL_CATEGORIZE(0,0).CATEGORY.EQ(\\"Malware\\")" -action AV_ACTION

set contentinspection policy

Modifies the rule, action or comment portion of the specified contentInspection policy.

Synopsis

set contentinspection policy <name>

Arguments

name Name of the contentInspection policy.

rule Expression that the policy uses to determine whether to execute the specified action.

action Name of the contentInspection action to perform if the request matches this contentInspection policy. There are also some built-in actions which can be used. These are:

- NOINSPECTION - Send the request from the client to the server or response from the server to the client without sending it to Inspection device for Content Inspection.
- RESET - Resets the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend the request if desired.
- DROP - Drop the request without sending a response to the user.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

comment Any type of information about this contentInspection policy.

logAction Name of the messagelog action to use for requests that match this policy.

Example

set contentInspection policy pol9 -rule "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh2\\")"

stat contentinspection policy

Displays statistics for all contentInspection policies currently configured on the Citrix ADC, or detailed statistics for the specified policy.

Synopsis

stat contentinspection policy

Arguments

name Name of the contentInspection policy for which to show detailed statistics.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Policy undef hits (Undefhits) Number of undef hits on the policy

Related Commands

- stat contentinspection policylabel

rm contentinspection policy

Removes the specified contentInspection policy.

Synopsis

rm contentinspection policy <name>

Arguments

name Name of the contentInspection policy to remove.

Example

rm contentInspection policy pol9

unset contentinspection policy

Removes the settings of an existing contentInspection policy. Attributes for which a default value is available revert to their default values. See the set contentInspection policy command for descriptions of the parameters..Refer to the set contentinspection policy command for meanings of the arguments.

Synopsis

unset contentinspection policy <name>

Example

unset contentInspection policy pol9 -undefAction

show contentinspection policy

Displays the current settings for the specified contentInspection policy. If no policy name is specified, displays a list of all contentInspection policies currently configured on the Citrix ADC, with abbreviated settings.

Synopsis

show contentinspection policy show contentinspection policy stats - alias for 'stat contentinspection policy'

Arguments

name Name of the contentInspection policy for which to display settings.

Output

stateflag rule Rule of the policy.

action CI action associated with the policy.

undefAction UNDEF action associated with the policy.

hits Number of hits.

undefHits Number of policy UNDEF hits.

activePolicy Indicates whether policy is bound or not.

boundTo Location where policy is bound

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

comment Any type of information about this contentInspection policy.

logAction Name of the messagelog action to use for requests that match this policy.

bindPolicyType vserverType builtin Flag to determine if contentInspection policy is built-in or not

feature The feature to be checked while applying this config

type devno count

Example

show contentInspection policy

contentinspection-policylabel

The following operations can be performed on "contentinspection-policylabel":

stat| rm| rename| bind| unbind| show| add|

stat contentinspection policylabel

Displays statistics for the specified contentInspection policy label. If no policy label name is provided, displays abbreviated statistics for all contentInspection policy labels currently configured on the Citrix ADC.

Synopsis

stat contentinspection policylabel

Arguments

labelName Name of the contentInspection policy label.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy Label Hits (Hits) Number of times policy label was invoked.

rm contentinspection policylabel

Removes the specified contentInspection policy label.

Synopsis

rm contentinspection policylabel <labelName>

Arguments

labelName Name of the contentInspection policy label to remove.

Example

rm contentInspection policylabel trans_http_url

rename contentinspection policylabel

Renames a contentInspection policy label.

Synopsis

rename contentinspection policylabel <labelName>@ <newName>@

Arguments

labelName Current name of the policy label.

newName New name for the contentInspection policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy label" or 'my policy label').

Example

rename contentInspection policylabel oldname newname

bind contentinspection policylabel

Binds the specified contentInspection policy to the specified policy label.

Synopsis

bind contentinspection policylabel <labelName> -policyName <string> -priority <positive_integer>

Arguments

labelName Name of the contentInspection policy label to which to bind the policy.

policyName Name of the contentInspection policy to bind to the policy label.

priority Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Must be unique within the label. Policies are evaluated in the order of their priorities, and the first policy that matches the request or response is applied. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:

- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.
- The expression evaluates to a priority number that is smaller than the current policyÂ’s priority number.
- The expression evaluates to a priority number that is between the current policyÂ’s priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

invoke Suspend evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

labelType Type of invocation. Available settings function as follows:

- reqvserver - Forward the request to the specified request virtual server.
- resvserver - Forward the response to the specified response virtual server.
- policylabel - Invoke the specified policy label.

Possible values: reqvserver, resvserver, policylabel

labelName

- If labelType is policylabel, name of the policy label to invoke.
- If labelType is reqvserver or resvserver, name of the virtual server to which to forward the request or response.

Example

i) bind contentInspection policylabel trans_http_url -policyName cipol2 -priority 1 -labelType reqvserver ii)bind contentInspection policylabel trans_http_url pol_2 2

unbind contentinspection policylabel

Unbinds the specified contentInspection policy from the specified policy label. See the bind contentInspection policylabel command for a description of the parameters.

Synopsis

unbind contentinspection policylabel <labelName> -policyName <string>

Arguments

labelName Name for the contentInspection policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the contentInspection policy label is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my contentInspection policy label" or 'my contentInspection policy label').

policyName Name of the contentInspection policy to bind to the policy label.

priority Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind contentInspection policylabel trans_http_url pol_1

show contentinspection policylabel

Displays the current settings for the specified contentInspection policy label. If no policy label is specified, displays a list of all contentInspection policy labels currently configured on the Citrix ADC.

Synopsis

show contentinspection policylabel

Arguments

labelName Name of the contentInspection policy label.

Output

stateflag type Type of packets (request or response packets) against which to match the policies bound to this policy label.

numpol Number of polices bound to label.

hits Number of times policy label was invoked.

policyName Name of the contentInspection policy to bind to the policy label.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke Suspend evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

labelType Type of invocation. Available settings function as follows:

- reqvserver - Forward the request to the specified request virtual server.
- resvserver - Forward the response to the specified response virtual server.
- policylabel - Invoke the specified policy label.

labelName

- If labelType is policylabel, name of the policy label to invoke.
- If labelType is reqvserver or resvserver, name of the virtual server to which to forward the request or response.

flowType Flowtype of the bound contentInspection policy.

isDefault A value of true is returned if it is a default cipolicylabel.

flags comment Any comments to preserve information about this contentInspection policy label.

devno count

Example

i)show contentInspection policylabel trans_http_url ii)show contentInspection policylabel

add contentinspection policylabel

Creates a user-defined contentInspection policy label.

Synopsis

add contentinspection policylabel <labelName> -type (REQ | RES)

Arguments

labelName Name for the contentInspection policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the contentInspection policy label is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my contentInspection policy label" or 'my contentInspection policy label').

type Type of packets (request or response packets) against which to match the policies bound to this policy label.

Possible values: REQ, RES

comment Any comments to preserve information about this contentInspection policy label.

Example

add contentInspection policylabel trans_http_url -type req

contentinspection-profile

The following operations can be performed on "contentinspection-profile":

unset| set| show| rm| add|

unset contentinspection profile

Use this command to remove contentinspection profile settings.Refer to the set contentinspection profile command for meanings of the arguments.

Synopsis

unset contentinspection profile <name>

set contentinspection profile

Modifies the attributes of contentinspection profile

Synopsis

set contentinspection profile <name>

Arguments

name Name of a ContentInspection profile. Must begin with a letter, number, or the underscore \(_\) character. Other characters allowed, after the first character, are the hyphen \(-\), period \(.\), hash \(#\), space \(\), at \(@\), colon \(:\), and equal \(=\) characters. The name of a IPS profile cannot be changed after it is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my ips profile" or 'my ips profile'\).

egressInterface Egress interface for CI profile.It is a mandatory argument while creating an ContentInspection profile of type INLINEINSPECTION or MIRROR.

ingressInterface Ingress interface for CI profile.It is a mandatory argument while creating an ContentInspection profile of IPS type.

egressVlan Egress Vlan for CI Minimum value: 0

ingressVlan Ingress Vlan for CI Minimum value: 0

ipTunnel IP Tunnel for CI profile. It is used while creating a ContentInspection profile of type MIRROR when the IDS device is in a different network

Example

set contentinspectionprofile <profile-name> -ingressinterface "1/3"

show contentinspection profile

Displays contentinspection profile/s configured on netscaler

Synopsis

show contentinspection profile

Arguments

name Name of the contentinspection profile to be displayed

Output

type Type of ContentInspection profile. Following types are available to configure: INLINEINSPECTION : To inspect the packets/requests using IPS. MIRROR : To forward cloned packets.

egressInterface Egress interface for CI profile.It is a mandatory argument while creating an ContentInspection profile of type INLINEINSPECTION or MIRROR.

ingressInterface Ingress interface for CI profile.It is a mandatory argument while creating an ContentInspection profile of IPS type.

egressVlan Egress Vlan for CI

ingressVlan Ingress Vlan for CI

ipTunnel IP Tunnel for CI profile. It is used while creating a ContentInspection profile of type MIRROR when the IDS device is in a different network

devno count stateflag

Example

show contentinspection profile

rm contentinspection profile

Removes contentinspection profile.

Synopsis

rm contentinspection profile <name>

Arguments

name Name of a ContentInspection profile. Must begin with a letter, number, or the underscore \(_\) character. Other characters allowed, after the first character, are the hyphen \(-\), period \(.\), hash \(#\), space \(\), at \(@\), colon \(:\), and equal \(=\) characters. The name of a IPS profile cannot be changed after it is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my ips profile" or 'my ips profile'\).

Example

rm contentinspectionprofile <profile-name>

add contentinspection profile

Adds ContentInspection profile to the NetScaler appliance.

Synopsis

add contentinspection profile <name> -type (InlineInspection | Mirror) [-ingressInterface <interface_name>] ((-egressInterface <interface_name>) | -ipTunnel <string>)

Arguments

name Name of a ContentInspection profile. Must begin with a letter, number, or the underscore \(_\) character. Other characters allowed, after the first character, are the hyphen \(-\), period \(.\), hash \(#\), space \(\), at \(@\), colon \(:\), and equal \(=\) characters. The name of a IPS profile cannot be changed after it is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my ips profile" or 'my ips profile'\).

type Type of ContentInspection profile. Following types are available to configure: INLINEINSPECTION : To inspect the packets/requests using IPS. MIRROR : To forward cloned packets.

Possible values: InlineInspection, Mirror

ingressInterface Ingress interface for CI profile.It is a mandatory argument while creating an ContentInspection profile of IPS type.

ingressVlan Ingress Vlan for CI Minimum value: 0

egressInterface Egress interface for CI profile.It is a mandatory argument while creating an ContentInspection profile of type INLINEINSPECTION or MIRROR.

ipTunnel IP Tunnel for CI profile. It is used while creating a ContentInspection profile of type MIRROR when the IDS device is in a different network

egressVlan Egress Vlan for CI Minimum value: 0

Example

add contentinspectionprofile ips_profile1 -type InlineInspection -ingressinterface "1/2" -egressinterface "1/4"

Contentinspection

The entities on which you can perform NetScaler CLI operations:

- contentinspection-action

- contentinspection-callout
- contentinspection
- contentinspection-global
- contentinspection-parameter
- contentinspection-policy
- contentinspection-policylabel
- contentinspection-profile
- contentinspection-stats

contentinspection-stats

The following operations can be performed on "contentinspection-stats":

show contentinspection stats

show contentinspection stats is an alias for stat contentinspection

Synopsis

show contentinspection stats - alias for 'stat contentinspection'

contentinspection

The following operations can be performed on "contentinspection":

stat contentinspection

Shows Content Inspection statistics.

Synopsis

stat contentinspection

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

requests (reqs) HTTP/HTTPS requests sent for ContentInspection.

responses (res) HTTP/HTTPS responses sent for ContentInspection.

Request Bytes Sent (reqBytesSent) Number of bytes transfered for requests to IPS

Request Bytes Received (reqBytesRecv) Number of bytes received for requests from IPS

Response Bytes Sent (respBytesSent) Number of bytes transfered for responses to IPS

Response Bytes Received (respBytesRecv) Number of bytes received for responses from IPS

Serverdown Reset Action taken (serverdownReset) Number of requests Reset when Inline device is down

Serverdown Drop Action taken (serverdownDrop) Number of requests Dropped when Inline device is down

Serverdown BYPASS Action taken (serverdownBypass) Number of requests bypass content Inspection Module when Inline device is down

Inline device Generated Responses (InlineDeviceResponses) Number of Inline device generated Responses

requests Sent (mirrorreqSent) Number of requests sent for Intrusion Detection

responses Sent (mirrorrespSent) Number of responses sent for Intrusion Detection

requests Bytes Sent (mirrorreqBytesSent) Number of request Bytes sent for Intrusion Detection

responses Bytes Sent (mirrorrespBytesSent) Number of response Bytes sent for Intrusion Detection

Serverdown Reset Action taken (serverdownReset) Number of requests Reset when Mirror device is down

Serverdown Drop Action taken (serverdownDrop) Number of requests Dropped when Mirror device is down

Serverdown BYPASS Action taken (serverdownBypass) Number of requests bypass ContentInspection module when Mirror device is down

REQMOD requests Sent (ICAPreqmodreqSent) Number of requests sent to ICAP Server

RESPMOD requests Sent (ICARespmodreqsSent) Number of responses sent for Intrusion DEtection

Preview Enabled requests (ICAPprevrequests) Number of preview requests for ICAP

204 Enabled Requests (204nocontetrequests) Number of 204 Rquests

100 Continue Responses Received (100contrecv) Number of 100-continue responses received

204 NO content Received (204NOcontentrecv) Number of 204 No content responses received

Adaptive Requests (adaptedreq) Number of Adaptive requests

Adaptive Responses (adaptedresp) Number of Adaptive Responses

Callout requests Initiated (Calloutinitiated) Number of callout Requests started

Callout requests completed (Calloutcomplete) Number of callout requests finished

ICAP Req/Resp Errors handled (errorsent) Number of errors sent

Serverdown Reset Action taken (serverdownReset) Number of requests for which serverdown Reset Action is taken

Serverdown Drop Action taken (serverdownDrop) Number of requests for which serverdown Drop Action is taken

Serverdown BYPASS Action taken (serverdownBypass) Number of requests for which serverdown Bypass Action is taken

Related Commands

- stat contentinspection policylabel

cr

cr-action

The following operations can be performed on "cr-action":

show cr action

Displays information about all the built-in or user defined cache redirection actions.

Synopsis

show cr action

Arguments

name Name of the action for which to display detailed information.

Output

crType Type to decide where to redirect the requests if the cache redirection policy is hit. The valid options are as follows: *CACHE - Directs all the requests to the cache if cache redirection policy is hit. *ORIGIN - Directs all requests to the origin server if the cache redirection policy is hit.

stateflag builtin Flag to determine whether CRACTION is default or not.

feature The feature to be checked while applying this config

isDefault A value of true is returned if it is a default cr action.

hits The number of times the action has been taken.

referenceCount The number of references to the action.

undefHits The number of times the action resulted in UNDEF.

comment Comment. Any type of information about this responder action.

devno count

Cr

The entities on which you can perform NetScaler CLI operations:

- cr-action
- cr-policy
- cr-vserver

cr-policy

The following operations can be performed on "cr-policy":

rm| add| unset| set| rename| show|

rm cr policy

Removes a cache redirection policy. You can delete a user-defined cache redirection policy that is not bound to a cache redirection virtual server. If the policy is bound to a virtual server, you must first unbind the policy, and then remove it.

Synopsis

rm cr policy <policyName>

Arguments

policyName Name of the cache redirection policy to remove.

Related Commands

- unset cr vserver

add cr policy

Creates a cache redirection policy. To associate the new policy with a cache redirection virtual server, use the bind cr vserver command.

Synopsis

add cr policy <policyName> -rule <expression>

Arguments

policyName Name for the cache redirection policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after the policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

rule Expression, or name of a named expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the built-in cache redirection action: CACHE/ORIGIN.

logAction The log action associated with the cache redirection policy

Related Commands

- unset cr vserver

unset cr policy

Unset logaction for existing cache redirection policy..Refer to the set cr policy command for meanings of the arguments.

Synopsis

unset cr policy <policyName> -logAction

Example

unset cr policy pol -logAction

set cr policy

Changes the specified parameters of an existing cache redirection policy.

Synopsis

set cr policy <policyName>

Arguments

policyName Name of the cache redirection policy to change.

rule Expression, or name of a named expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action The cache redirection action name.

logAction The log action associated with the cache redirection policy

rename cr policy

Rename a cache redirection policy.

Synopsis

rename cr policy <policyName>@ <newName>@

Arguments

policyName The name of the content switching policy.

newName The new name of the content switching policy.

Example

rename cr policy oldname newname

show cr policy

Displays all existing cache redirection policies, or just the specified policy.

Synopsis

show cr policy

Arguments

policyName Name of the cache redirection policy to display. If this parameter is omitted, details of all the policies are displayed.

Output

rule Expression, or name of a named expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

boundTo Domain name.

action The CR action name.

vstype Virtual server type.

hits Total number of hits.

bindHits Total number of hits.

priority priority of bound policy

flag stateflag activePolicy Indicates whether policy is bound or not.

logAction The log action associated with the cache redirection policy

labelName Name of the label invoked.

labelType The invocation type.

builtin feature The feature to be checked while applying this config

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

isDefault A value of true is returned if it is a default cr policy.

devno count

Related Commands

- unset cr vserver

cr-vserver

The following operations can be performed on "cr-vserver":

bind| rm| add| stat| rename| set| disable| unset| show| unbind| enable|

bind cr vserver

Binds a cache redirection policy to a cache redirection virtual server.

Synopsis

bind cr vserver <name> (-lbvserver <string> | (-policyName <string>) | <targetVserver> | -analyticsProfile <string>)

Arguments

name Name of the cache redirection virtual server to which to bind the cache redirection policy.

lbvserver Name of the virtual server to which content is forwarded. Applicable only if the policy is a map policy and the cache redirection virtual server is of type REVERSE.

policyName Name of the cache redirection policy that you are binding.

targetVserver Name of the virtual server to which content is forwarded. Applicable only if the policy is a map policy and the cache redirection virtual server is of type REVERSE.

priority An unsigned integer that determines the priority of the policy relative to other policies bound to this cache redirection virtual server. The lower the value, higher the priority. Note: This option is available only when binding content switching, filtering, and compression policies to a cache redirection virtual server. Minimum value: 0

gotoPriorityExpression Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.

- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), b ut does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number incr ements by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

type For a rewrite policy, the bind point to which to bind the policy. Note: This parameter applies only to rewrite policies, because content switching policies are evaluated only at request time.

Possible values: REQUEST, RESPONSE, ICA_REQUEST

invoke Invoke a policy label if this policy's rule evaluates to TRUE.

labelType Type of label to be invoked.

Possible values: reqvserver, resvserver, policylabel

labelName Name of the label to be invoked.

analyticsProfile Bind an analytics profile to a CR vserver.

rm cr vserver

Removes a virtual server.

Synopsis

rm cr vserver <name>@ ...

Arguments

name Name of the virtual server to be removed.

Example

rm vserver cr_vip

add cr vserver

Creates a cache redirection virtual server.

Synopsis

add cr vserver <name> <serviceType> [-cacheType <cacheType>] [-Listenpolicy <expression>] [-probeProtocol (TCP | HTTP)]

Arguments

name Name for the cache redirection virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the cache redirection virtual server is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my server" or 'my server').

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

serviceType Protocol (type of service) handled by the virtual server.

Possible values: HTTP, SSL, NNTP, HDX

IPAddress IPv4 or IPv6 address of the cache redirection virtual server. Usually a public IP address. Clients send connection requests to this IP address. Note: For a transparent cache redirection virtual server, use an asterisk (*) to specify a wildcard virtual server address.

port Port number of the virtual server. Default value: 80 Minimum value: 1 Maximum value: 65534

ipset The list of IPv4/IPv6 addresses bound to ipset would form a part of listening service on the current cr vserver

range Number of consecutive IP addresses, starting with the address specified by the IPAddress parameter, to include in a range of addresses assigned to this virtual server. Default value: 1 Minimum value: 1 Maximum value: 254

cacheType Mode of operation for the cache redirection virtual server. Available settings function as follows:

- TRANSPARENT - Intercept all traffic flowing to the appliance and apply cache redirection policies to determine whether content should be served from the cache or from the origin server.
- FORWARD - Resolve the hostname of the incoming request, by using a DNS server, and forward requests for non-cacheable content to the resolved origin servers. Cacheable requests are sent to the configured cache servers.
- REVERSE - Configure reverse proxy caches for specific origin servers. Incoming traffic directed to the reverse proxy can either be served from a cache server or be sent to the origin server with or without modification to the URL. The default value for cache type is TRANSPARENT if service is HTTP or SSL whereas the default cache type is FORWARD if the service is HDX.

Possible values: TRANSPARENT, REVERSE, FORWARD

redirect Type of cache server to which to redirect HTTP requests. Available settings function as follows:

- CACHE - Direct all requests to the cache.
- POLICY - Apply the cache redirection policy to determine whether the request should be directed to the cache or to the origin.
- ORIGIN - Direct all requests to the origin server.

Possible values: CACHE, POLICY, ORIGIN Default value: POLICY

onPolicyMatch Redirect requests that match the policy to either the cache or the origin server, as specified. Note: For this option to work, you must set the cache redirection type to POLICY.

Possible values: CACHE, ORIGIN Default value: ORIGIN

redirectURL URL of the server to which to redirect traffic if the cache redirection virtual server configured on the Citrix ADC becomes unavailable.

cltTimeout Time-out value, in seconds, after which to terminate an idle client connection. Maximum value: 31536000

arp Use ARP to determine the destination MAC address.

Possible values: ON, OFF

map Obsolete.

Possible values: ON, OFF

format via Insert a via header in each HTTP request. In the case of a cache miss, the request is redirected from the cache server to the origin server. This header indicates whether the request is being sent from a cache server.

Possible values: ON, OFF Default value: ON

dnsVserverName Name of the DNS virtual server that resolves domain names arriving at the forward proxy virtual server. Note: This parameter applies only to forward proxy virtual servers, not reverse or transparent.

destinationVServer Destination virtual server for a transparent or forward proxy cache redirection virtual server.

domain Default domain for reverse proxies. Domains are configured to direct an incoming request from a specified source domain to a specified target domain. There can be several configured pairs of source and target domains. You can select one pair to be the default. If the host header or URL of an incoming request does not include a source domain, this option sends the request to the specified target domain.

soPersistenceTimeOut Time-out, in minutes, for spillover persistence. Minimum value: 2 Maximum value: 24

soThreshold For CONNECTION (or) DYNAMICCONNECTION spillover, the number of connections above which the virtual server enters spillover mode. For BANDWIDTH spillover, the amount of incoming and outgoing traffic (in Kbps) before spillover. For HEALTH spillover, the percentage of active services (by weight) below which spillover occurs. Minimum value: 1

reuse Reuse TCP connections to the origin server across client connections. Do not set this parameter unless the Service Type parameter is set to HTTP. If you set this parameter to OFF, the possible settings of the Redirect parameter function as follows:

- CACHE - TCP connections to the cache servers are not reused.

- ORIGIN - TCP connections to the origin servers are not reused.
- POLICY - TCP connections to the origin servers are not reused. If you set the Reuse parameter to ON, connections to origin servers and connections to cache servers are reused.

Possible values: ON, OFF Default value: ON

state Initial state of the cache redirection virtual server.

Possible values: ENABLED, DISABLED Default value: ENABLED

downStateFlush Perform delayed cleanup of connections to this virtual server.

Possible values: ENABLED, DISABLED Default value: ENABLED

backupVServer Name of the backup virtual server to which traffic is forwarded if the active server becomes unavailable.

disablePrimaryOnDown Continue sending traffic to a backup virtual server even after the primary virtual server comes UP from the DOWN state.

Possible values: ENABLED, DISABLED Default value: DISABLED

l2Conn Use L2 parameters, such as MAC, VLAN, and channel to identify a connection.

Possible values: ON, OFF

backendssl Decides whether the backend connection made by Citrix ADC to the origin server will be HTTP or SSL. Applicable only for SSL type CR Forward proxy vserver.

Possible values: ENABLED, DISABLED Default value: DISABLED

Listenpolicy String specifying the listen policy for the cache redirection virtual server. Can be either an in-line expression or the name of a named expression. Default value: "NONE"

Listenpriority Priority of the listen policy specified by the Listen Policy parameter. The lower the number, higher the priority. Default value: 101 Minimum value: 0 Maximum value: 100

tcpProfileName Name of the profile containing TCP configuration information for the cache redirection virtual server.

httpProfileName Name of the profile containing HTTP configuration information for cache redirection virtual server.

comment Comments associated with this virtual server.

srcIPExpr Expression used to extract the source IP addresses from the requests originating from the cache. Can be either an in-line expression or the name of a named expression.

originUSIP Use the client's IP address as the source IP address in requests sent to the origin server. Note: You can enable this parameter to implement fully transparent CR deployment.

Possible values: ON, OFF Default value: VAL_NOT_SET

usePortRange Use a port number from the port range (set by using the set ns param command, or in the Create Virtual Server (Cache Redirection) dialog box) as the source port in the requests sent to the origin server.

Possible values: ON, OFF Default value: OFF

appflowLog Enable logging of AppFlow information.

Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile Name of the network profile containing network configurations for the cache redirection virtual server.

icmpVsrResponse Criterion for responding to PING requests sent to this virtual server. If ACTIVE, respond only if the virtual server is available. If PASSIVE, respond even if the virtual server is not available.

Possible values: PASSIVE, ACTIVE Default value: PASSIVE

RHIstate A host route is injected according to the setting on the virtual servers

- If set to PASSIVE on all the virtual servers that share the IP address, the appliance always injects the hostroute.
- If set to ACTIVE on all the virtual servers that share the IP address, the appliance injects even if one virtual server is UP.
- If set to ACTIVE on some virtual servers and PASSIVE on the others, the appliance, injects even if one virtual server set to ACTIVE is UP.

Possible values: PASSIVE, ACTIVE Default value: PASSIVE

UseOriginIpPortForCache Use origin ip/port while forwarding request to the cache. Change the destination IP, destination port of the request came to CR vserver to Origin IP and Origin Port and forward it to Cache

Possible values: YES, NO Default value: NO

probeProtocol Citrix ADC provides support for external health check of the vserver status. Select HTTP or TCP probes for healthcheck

Possible values: TCP, HTTP

probeSuccessResponseCode HTTP code to return in SUCCESS case. Default value: "200 OK"

probePort Citrix ADC provides support for external health check of the vserver status. Select port for HTTP/TCP monitring Default value: 0

disallowServiceAccess This is effective when a FORWARD type cr vserver is added. By default, this parameter is DISABLED. When it is ENABLED, backend services cannot be accessed through a FORWARD type cr vserver.

Possible values: ENABLED, DISABLED Default value: DISABLED

Related Commands

- show policy expression

stat cr vserver

Displays statistics for all cache redirection virtual servers or for the cache redirection virtual server specified by the name parameter.

Synopsis

stat cr vserver

Arguments

name Name of a specific cache redirection virtual server.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

IP address (IP) The IP address on which the service is running.

Port (port) The port on which the service is running.

Vserver protocol (Protocol) Protocol associated with the vserver

State Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)

Vserver hits (Hits) Total vserver hits

Requests (Req) Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Responses (Rsp) Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Request bytes (Reqb) Total number of request bytes received on this service or virtual server.

Response bytes (Rspb) Number of response bytes received by this service or virtual server.

Total Packets rcvd (PktRx) Total number of packets received by this service or virtual server.

Total Packets sent (PktTx) Total number of packets sent.

Invalid Request/Response (IvldReqRsp) Number invalid requests/responses on this vserver

Invalid Request/Response Dropped (IvldReqRspDrp) Number invalid requests/responses dropped on this vserver

rename cr vserver

Renames a cache redirection virtual server.

Synopsis

rename cr vserver <name>@ <newName>@

Arguments

name Existing name of the cache redirection virtual server.

newName New name for the cache redirection virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my name" or 'my name').

Example

rename cr vserver vscr1 vscrnew

set cr vserver

Changes the specified settings of the cache redirection virtual server.

Synopsis

set cr vserver <name> [-probeProtocol (TCP | HTTP)]

Arguments

name Name of the cache redirection virtual server.

IPAddress New IPv4 or IPv6 address of the cache redirection virtual server. Usually a public IP address. Clients send connection requests to this IP address.

ipset The list of IPv4/IPv6 addresses bound to ipset would form a part of listening service on the current cr vserver

redirect Type of server to which to redirect HTTP requests. Available settings function as follows: *CACHE - Direct all requests to the cache.*POLICY - Apply the cache redirection policy to determine whether the request should be directed to the cache or to the origin.*ORIGIN - Direct all requests to the origin server.

Possible values: CACHE, POLICY, ORIGIN Default value: POLICY

onPolicyMatch Redirect requests that match the policy to either the cache or the origin server, as specified. Note: For this option to work, you must set the cache redirection type to POLICY.

Possible values: CACHE, ORIGIN Default value: ORIGIN

arp Use ARP to determine the destination MAC address. Specify OFF to use the incoming destination MAC address, or ON to use ARP to determine the destination MAC address.

Possible values: ON, OFF

via Insert a via header in each HTTP request. In the case of a cache miss, the request is redirected from the cache server to the origin server. This header indicates whether the request is being sent from a cache server.

Possible values: ON, OFF Default value: ON

dnsVserverName Name of the DNS virtual server that resolves domain names arriving at the forward proxy virtual server. Note: This parameter applies only to forward proxy virtual servers, not reverse or transparent.

destinationVServer Destination virtual server for a transparent or forward proxy cache redirection virtual server.

domain Default domain for reverse proxies. Domains are configured to direct incoming requests from a specified source domain to a specified target domain. There can be several configured pairs of source and target domains. You can select one pair to be the default. If the host header or URL of an incoming request does not include a source domain, this option sends the request to the specified target domain.

reuse Reuse TCP connections to the origin server across client connections

Possible values: ON, OFF Default value: ON

backupVServer Name of the backup virtual server to which traffic is forwarded if the active server becomes unavailable.

disablePrimaryOnDown Continue sending traffic to a backup virtual server even after the primary virtual server comes UP from the DOWN state.

Possible values: ENABLED, DISABLED Default value: DISABLED

redirectURL URL of the server to which to redirect traffic if the cache redirection virtual server in the Citrix ADC becomes unavailable.

cltTimeout Time-out value, in seconds, after which an idle client connection is terminated. Maximum value: 31536000

downStateFlush Perform delayed cleanup of connections to this virtual server.

Possible values: ENABLED, DISABLED Default value: ENABLED

l2Conn Use L2 parameters, such as MAC, VLAN, and channel to identify a connection.

Possible values: ON, OFF

backendssl Decides whether the backend connection made by Citrix ADC to the origin server will be HTTP or SSL. Applicable only for SSL type CR Forward proxy vserver.

Possible values: ENABLED, DISABLED Default value: DISABLED

Listenpolicy String specifying the listen policy for the cache redirection virtual server. Can be either an in-line expression or the name of a named expression. Default value: "NONE"

Listenpriority Priority of the listen policy specified by the Listen Policy parameter. The lower the number, higher the priority. Default value: 101 Minimum value: 0 Maximum value: 100

tcpProfileName Name of the profile containing TCP configuration information for the cache redirection virtual server.

httpProfileName Name of the profile containing HTTP configuration information for cache redirection virtual server.

netProfile Name of the network profile containing network configurations for the cache redirection virtual server.

comment Comments associated with this virtual server.

srcIPExpr Expression used to extract the source IP addresses from the requests originating from the cache. Can be either an in-line expression or the name of a named expression.

originUSIP Use the client's IP address as the source IP address in requests sent to the origin server. Note: You can enable this parameter to implement fully transparent CR deployment.

Possible values: ON, OFF Default value: VAL_NOT_SET

usePortRange Use a port number from the port range (set by using the set ns param command, or in the Create Virtual Server (Cache Redirection) dialog box) as the source port in the requests sent to the origin server.

Possible values: ON, OFF Default value: OFF

appflowLog Enable logging of AppFlow information.

Possible values: ENABLED, DISABLED Default value: ENABLED

icmpVsrResponse Criterion for responding to PING requests sent to this virtual server. If ACTIVE, respond only if the virtual server is available. If PASSIVE, respond even if the virtual server is not available.

Possible values: PASSIVE, ACTIVE Default value: PASSIVE

RHIstate A host route is injected according to the setting on the virtual servers

- If set to PASSIVE on all the virtual servers that share the IP address, the appliance always injects the hostroute.
- If set to ACTIVE on all the virtual servers that share the IP address, the appliance injects even if one virtual server is UP.
- If set to ACTIVE on some virtual servers and PASSIVE on the others, the appliance, injects even if one virtual server set to ACTIVE is UP.

Possible values: PASSIVE, ACTIVE Default value: PASSIVE

UseOriginIpPortForCache Use origin ip/port while forwarding request to the cache. Change the destination IP, destination port of the request came to CR vserver to Origin IP and Origin Port and forward it to Cache

Possible values: YES, NO Default value: NO

probeProtocol Citrix ADC provides support for external health check of the vserver status. Select HTTP or TCP probes for healthcheck

Possible values: TCP, HTTP

probeSuccessResponseCode HTTP code to return in SUCCESS case. Default value: "200 OK"

probePort Citrix ADC provides support for external health check of the vserver status. Select port for HTTP/TCP monitring Default value: 0

disallowServiceAccess This is effective when a FORWARD type cr vserver is added. By default, this parameter is DISABLED. When it is ENABLED, backend services cannot be accessed through a FORWARD type cr vserver.

Possible values: ENABLED, DISABLED Default value: DISABLED

disable cr vserver

Disables a cache redirection virtual server.

Synopsis

disable cr vserver <name>@

Arguments

name Name of the cache redirection virtual server to be disabled. (Because the virtual server is still configured, you can reenable it.) Note: The appliance still responds to ARP and ping requests sent to the IP address of this virtual server.

Example

disable vserver cr_vip

unset cr vserver

Restores the specified parameters of a cache redirection virtual server to their default values. To unset all except the Name parameter, do not specify a value for any other parameter. Refer to the set cr vserver command for a description of the parameters..Refer to the set cr vserver command for meanings of the arguments.

Synopsis

unset cr vserver <name>

Related Commands

- show cr policy

show cr vserver

Displays cache redirection virtual server information. To display information about all configured cache redirection virtual servers, do not include a parameter. To display detailed information about a specific virtual server, use the name parameter to specify the name of the virtual server.

Synopsis

show cr vserver

Arguments

name Name of a cache redirection virtual server about which to display detailed information.

Output

IPAddress td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

IPAddress The IP address of the virtual server.

stateflag value The ssl card status for the transparent ssl cr vserver.

port Port number of the virtual server.

range Number of consecutive IP addresses, starting with the address specified by the IP Address parameter, to include in a range of addresses assigned to this virtual server.

serviceType Protocol (type of service) handled by the virtual server.

ngname Nodegroup devno to which this crvserver belongs to

type Virtual server type.

vsvrcfgflags Contains the config info of vserver to be used at validation

state The state of the cr vserver.

status Status.

cacheType Mode of operation for the cache redirection virtual server. Available settings function as follows:

- TRANSPARENT - Intercept all traffic flowing to the appliance and apply cache redirection policies to determine whether content should be served from the cache or from the origin server.
- FORWARD - Resolve the hostname of the incoming request, by using a DNS server, and forward requests for non-cacheable content to the resolved origin servers. Cacheable requests are sent to the configured cache servers.
- REVERSE - Configure reverse proxy caches for specific origin servers. Incoming traffic directed to the reverse proxy can either be served from a cache server or be sent to the origin server with or without modification to the URL. The default value for cache type is TRANSPARENT if service is HTTP or SSL whereas the default cache type is FORWARD if the service is HDX.

redirect Type of cache server to which to redirect HTTP requests. Available settings function as follows:

- CACHE - Direct all requests to the cache.
- POLICY - Apply the cache redirection policy to determine whether the request should be directed to the cache or to the origin.
- ORIGIN - Direct all requests to the origin server.

onPolicyMatch Redirect requests that match the policy to either the cache or the origin server, as specified. Note: For this option to work, you must set the cache redirection type to POLICY.

precedence Type of policy (URL or RULE) that takes precedence on the cache redirection virtual server. Applies only to cache redirection virtual servers that have both URL and RULE based policies. If you specify URL, URL based policies are applied first, in the following order:

1. Domain and exact URL
2. Domain, prefix and suffix
3. Domain and suffix
4. Domain and prefix
5. Domain only
6. Exact URL
7. Prefix and suffix
8. Suffix only
9. Prefix only
10. Default If you specify RULE, the rule based policies are applied before URL based policies are applied.

redirectURL URL of the server to which to redirect traffic if the cache redirection virtual server configured on the Citrix ADC becomes unavailable.

authentication Authentication.

homePage Home page.

dnsVserverName Name of the DNS virtual server that resolves domain names arriving at the forward proxy virtual server. Note: This parameter applies only to forward proxy virtual servers, not reverse or transparent.

domain Default domain for reverse proxies. Domains are configured to direct an incoming request from a specified source domain to a specified target domain. There can be several configured pairs of source and target domains. You can select one pair to be the default. If the host header or URL of an incoming request does not include a source domain, this option sends the request to the specified target domain.

rule Rule.

policyName Policies bound to this vserver.

piPolicyhits Number of hits.

hits Number of hits.

serviceName Service name.

weight Weight for this service.

cacheVserver Name of the default cache virtual server to which to redirect requests (the default target of the cache redirection virtual server).

targetVserver The CSW target server names.

backupVServer Name of the backup virtual server to which traffic is forwarded if the active server becomes unavailable.

priority The priority for the policy.

cltTimeout Time-out value, in seconds, after which to terminate an idle client connection.

soMethod The spillover factor. When the main virtual server reaches this spillover threshold, it will give further traffic to the backupvserver.

soPersistence The state of spillover persistence.

soPersistenceTimeOut The spillover persistence entry timeout.

soThreshold The spillover threshold value.

reuse Reuse TCP connections to the origin server across client connections. Do not set this parameter unless the Service Type parameter is set to HTTP. If you set this parameter to OFF, the possible settings of the Redirect parameter function as follows:

- CACHE - TCP connections to the cache servers are not reused.

- ORIGIN - TCP connections to the origin servers are not reused.
- POLICY - TCP connections to the origin servers are not reused. If you set the Reuse parameter to ON, connections to origin servers and connections to cache servers are reused.

arp destinationVServer Destination virtual server for a transparent or forward proxy cache redirection virtual server.

via Insert a via header in each HTTP request. In the case of a cache miss, the request is redirected from the cache server to the origin server. This header indicates whether the request is being sent from a cache server.

downStateFlush Perform delayed clean up of connections on this vserver.

disablePrimaryOnDown Tells whether traffic will continue reaching backup vservers even after primary comes UP from DOWN state.

l2Conn Use L2 parameters, such as MAC, VLAN, and channel to identify a connection.

backendssl Decides whether the backend connection made by Citrix ADC to the origin server will be HTTP or SSL. Applicable only for SSL type CR Forward proxy vserver.

comment Comments associated with this virtual server.

Listenpolicy The string is listenpolicy configured for CR vserver

Listenpriority This parameter is the priority for listen policy of CR Vserver.

tcpProfileName Name of the profile containing TCP configuration information for the cache redirection virtual server.

httpProfileName Name of the profile containing HTTP configuration information for cache redirection virtual server.

srcIPExpr Expression used to extract the source IP addresses from the requests originating from the cache. Can be either an in-line expression or the name of a named expression.

originUSIP Use the client's IP address as the source IP address in requests sent to the origin server. Note: You can enable this parameter to implement fully transparent CR deployment.

usePortRange Use a port number from the port range (set by using the set ns param command, or in the Create Virtual Server (Cache Redirection) dialog box) as the source port in the requests sent to the origin server.

appflowLog Enable logging of AppFlow information.

netProfile Name of the network profile containing network configurations for the cache redirection virtual server.

state Initial state of the cache redirection virtual server.

icmpVsrResponse Criterion for responding to PING requests sent to this virtual server. If ACTIVE, respond only if the virtual server is available. If PASSIVE, respond even if the virtual server is not available.

RHIstate A host route is injected according to the setting on the virtual servers

- If set to PASSIVE on all the virtual servers that share the IP address, the appliance always injects the hostroute.
- If set to ACTIVE on all the virtual servers that share the IP address, the appliance injects even if one virtual server is UP.
- If set to ACTIVE on some virtual servers and PASSIVE on the others, the appliance, injects even if one virtual server set to ACTIVE is UP.

lbvserver The Default target server name.

inherited On State describes that policy bound is inherited from global binding.

type The bindpoint to which the policy is bound

invoke Invoke flag.

labelType The invocation type.

labelName Name of the label invoked.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

ipset The list of IPv4/IPv6 addresses bound to ipset would form a part of listening service on the current cr vserver

noDefaultBindings to determine if the configuration will have default ssl CIPHER and ECC curve bindings

UseOriginIpPortForCache Use origin ip/port while forwarding request to the cache. Change the destination IP, destination port of the request came to CR vserver to Origin IP and Origin Port and forward it to Cache

tcpProbePort Port number for external TCP probe. NetScaler provides support for external TCP health check of the vserver status over the selected port. This option is only supported for vservers assigned with an IPAddress or ipset.

analyticsProfile Name of the analytics profile bound to the CR vserver.

probeProtocol Citrix ADC provides support for external health check of the vserver status. Select HTTP or TCP probes for healthcheck

probePort Citrix ADC provides support for external health check of the vserver status. Select port for HTTP/TCP monitring

probeSuccessResponseCode HTTP code to return in SUCCESS case.

disallowServiceAccess This is effective when a FORWARD type cr vserver is added. By default, this parameter is DISABLED. When it is ENABLED, backend services cannot be accessed through a FORWARD type cr vserver.

devno count

Related Commands

- show cs policy

unbind cr vserver

Unbinds a cache redirection policy from a cache redirection virtual server.

Synopsis

unbind cr vserver <name> ((-policyName <string>) | -lbvserver <string> | -analyticsProfile <string>)

Arguments

name Name of the cache redirection virtual server from which to unbind the policy.

policyName Name of the cache redirection policy that you are unbinding.

type For rewrite policies, the traffic flow to which the policy applies. Note: This parameter applies only to rewrite policies, because cache redirection policies are evaluated only at request time.

Possible values: REQUEST, RESPONSE, ICA_REQUEST

priority Priority number of the policy from which to unbind the content switching virtual server. Minimum value: 1

lbvserver The virtual server name (created with the add lb vserver command) to which content will be switched. Default value: "default_lb"

analyticsProfile Unbind an analytics profile from CR vserver.

Related Commands

- show cr policy

enable cr vserver

Enables a cache redirection virtual server. Note: Virtual servers, when added, are enabled by default.

Synopsis

enable cr vserver <name>@

Arguments

name Name of the cache redirection virtual server to be enabled.

Example

enable vserver cr_vip

cs

cs-action

The following operations can be performed on "cs-action":

show| set| rm| rename| add| unset|

show cs action

Displays the configuration settings of the specified content switching action or lists all the content switching actions configured on the appliance.

Synopsis

show cs action

Arguments

name Name of the content switching action.

Output

stateflag targetLBVserver Target LB vserver name.

targetVserver Target VPN vserver name.

targetVserverExpr Target LB vserver expression.

hits The number of times the action has been taken.

referenceCount The number of references to the action.

undefHits The number of times the action resulted in UNDEF.

builtin feature The feature to be checked while applying this config

comment Comments associated with this cs action.

gslbBindings devno count

Example

show cs action

set cs action

Modifies the configuration settings of a content switching action.

Synopsis

set cs action <name>

Arguments

name Name for the content switching action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the content switching action is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

targetLBVserver Name of the load balancing virtual server to which the content is switched.

targetVserver Name of the VPN, GSLB or Authentication virtual server to which the content is switched.

targetVserverExpr Information about this content switching action.

comment Comments associated with this cs action.

Example

set cs action act1 -targetLBVserver lb2 -comment 'for url'

rm cs action

Removes a content switching action.

Synopsis

rm cs action <name>

Arguments

name Name of the cs action.

Example

rm cs action act_before

rename cs action

Renames a content switching action.

Synopsis

rename cs action <name>@ <newName>@

Arguments

name Existing name of the content switching action.

newName New name for the content switching action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my name" or 'my name').

Example

rename cs action oldname newname

add cs action

Creates an action that indicates the target load balancing virtual server. This action is used to specify the target load balancing virtual server while defining a policy to support multiple policy bind support.

Synopsis

add cs action <name>

Arguments

name Name for the content switching action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the content switching action is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

targetLBVserver Name of the load balancing virtual server to which the content is switched.

targetVserver Name of the VPN, GSLB or Authentication virtual server to which the content is switched.

targetVserverExpr Information about this content switching action.

comment Comments associated with this cs action.

Example

i)When LB is the target: add cs action act1 -targetLBVserver lb1 ii)When VPN vserver is the target: add cs action act2 -targetVserver vpn1 iii)When GSLB vserver is the target: add cs action act2 -targetVserver gslb1 iv)Using expressions to extract the LB vserver: add cs action act3 -targetVserverExpr '"lbv"+CLIENT.TCP.CS_VSERVER.NAME.AFTER_STR("csv")'

unset cs action

Use this command to remove cs action settings.Refer to the set cs action command for meanings of the arguments.

Synopsis

unset cs action <name> -comment

Cs

The entities on which you can perform NetScaler CLI operations:

- cs-action
- cs-parameter
- cs-policy
- cs-policylabel
- cs-vserver

cs-parameter

The following operations can be performed on "cs-parameter":

set| unset| show|

set cs parameter

Sets the status of the state update parameter for the server. By default, the content switching virtual server is always UP, regardless of the state of the load balancing virtual servers bound to it. This command enables the virtual server to check the status of the attached load balancing server for state information.

Synopsis

set cs parameter -stateupdate (ENABLED | DISABLED)

Arguments

stateupdate Specifies whether the virtual server checks the attached load balancing server for state information.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set cs parameter -stateupdate (ENABLED|DISABLED)

unset cs parameter

Use this command to remove cs parameter settings.Refer to the set cs parameter command for meanings of the arguments.

Synopsis

unset cs parameter -stateupdate

show cs parameter

Show CS parameters

Synopsis

show cs parameter

Arguments

Output

stateupdate Specifies whether the virtual server checks the attached load balancing server for state information.

builtin Flag to determine if CS param is built-in or not

feature The feature to be checked while applying this config

Example

show cs parameter

cs-policy

The following operations can be performed on "cs-policy":

rm| rename| unset| set| add| show|

rm cs policy

Removes a content switching policy. You can delete a user-defined content switching policy that is not bound to a content switching virtual server. If the policy is bound to a virtual server, you must first unbind the policy, and then remove it.

Synopsis

rm cs policy <policyName>

Arguments

policyName Name of the content switching policy to be removed.

rename cs policy

Rename a content switching policy.

Synopsis

rename cs policy <policyName>@ <newName>@

Arguments

policyName The name of the content switching policy.

newName The new name of the content switching policy.

Example

rename cs policy oldname newname

unset cs policy

Unset logaction for existing content swtching policy..Refer to the set cs policy command for meanings of the arguments.

Synopsis

unset cs policy <policyName> -logAction

Example

unset cs policy pol9 -logAction

set cs policy

Changes an existing content switching policy.

Synopsis

set cs policy <policyName>

Arguments

policyName Name of the content switching policy.

rule The condition for applying this policy.

action The content switching action name.

logAction The log action associated with the content switching policy

add cs policy

Creates a new content switching policy. You use this policy to manage content switching on a virtual server.

Synopsis

add cs policy <policyName> -rule <expression>

Arguments

policyName Name for the content switching policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after a policy is created. The following requirement applies only to the Citrix ADC CLI: If the name

includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

rule Expression, or name of a named expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Content switching action that names the target load balancing virtual server to which the traffic is switched.

logAction The log action associated with the content switching policy

Example

To match the requests that have URL ".html", you would enter the following command: add cs policy <policyName> -rule http.req.url.eq(".html") -action <actionName> To match with all URLs that start with "/sports.html", you would enter the following command: add cs policy <policyName> -rule http.req.url.startswith("/sports.html") -action <actionName> To match requests with the URL "/sports/tennis/index.html", you would enter the following command: add cs policy <policyName> -rule http.req.url.eq("/sports/tennis/index.html") -action <actionName> To match requests that have URLs with the extension "jsp", you would enter the following command: add cs policy <policyName> -rule http.req.url.suffix.eq("jsp") -action <actionName> To match requests with URLs that start with "/sports.html" and the file extension "jsp", you would enter the following command: add cs policy <policyName> -rule "http.req.url.startswith(\"/sports/\") && http.req.url.suffix.eq(\"jsp\")" -action <actionName> To match requests with URLs that contain "sports", you would enter the following commands: add pol expression sports_url http.req.url.contains("sports") add cs policy <policyName> -rule sports_url -action <actionName> To match requests with URL queries that contain "gold" or cookie headers that contain "gold", you would enter the following commands: add pol expression gold_query "http.req.url.query.contains(\"gold\")" add pol expression gold_cookie "http.req.header(\"cookie\").contains(\"gold\")" add cs policy <policyName> -rule "(gold_query || gold_cookie)" -action <actionName> To match requests with the domain name www.domainxyz.com, you enter the following command: add cs policy <policyName> -rule "http.req.hostname.eq(\"www.domainxyz.com\")" -action <actionName> To match requests with the

domain name www.domainxyz.com and URLs with the extension "jsp", you would enter the following command: add cs policy <policyName> -rule "http.req.hostname.eq(\"www.domainxyz.com\") && http.req.url.suffix.eq(\"jsp\")" -action <actionName> To match requests with the domain name www.domainxyz.com and URLs that contain "sports", you would enter the following commands: add pol expression sports_url http.req.url.contains("sports") add cs policy <policyName> -rule "sports_url && http.req.hostname.eq(\"www.domainxyz.com\")" -action <actionName> To match a policy with a rule and provide action: add cs policy <policyname> -rule "http.req.method.eq(GET)" -action <actionName>

show cs policy

Displays all existing content switching policies, or just the specified policy.

Synopsis

show cs policy

Arguments

policyName Name of the content switching policy to display. If this parameter is omitted, details of all the policies are displayed.

Output

rule The condition for applying this policy.

action The CS action name.

vstype Virtual server type.

hits Total number of hits.

bindHits Total number of bind hits.

labelName Name of the label invoked.

labelType The invocation type.

target Target flag

priority priority of bound policy

flag stateflag activePolicy Indicates whether policy is bound or not.

logAction The log action associated with the content switching policy

gslbBindings boundTo Location where policy is bound

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

devno count

Related Commands

- show cs vserver

cs-policylabel

The following operations can be performed on "cs-policylabel":

bind| rm| rename| show| unbind| add|

bind cs policylabel

Binds a content switching policy to a content switching policy label.

Synopsis

bind cs policylabel <labelName> <policyName> <priority>

Arguments

labelName Name of the policy label to which to bind a content switching policy.

policyName Name of the content switching policy to bind to the content switching policy label.

priority Unsigned integer that determines the priority of the policy relative to other policies in this policy label. Smaller the number, higher the priority. Minimum value: 1 Maximum value: 2147483647

targetVserver Name of the virtual server to which to forward requests that match the policy.

gotoPriorityExpression Expression or other value specifying the priority of the next policy to be evaluated if the current policy rule evaluates to TRUE. Alternatively, you can specify one of the following values:

- NEXT - Go to the policy with the next higher priority.

- END - End evaluation. (This is the default. Evaluation stops if the gotoPriorityExpression parameter is not set.)
- USE_INVOCATION_RESULT - Applicable if this entry invokes another policy label. If the final goto in the invoked policy label has a value of END, evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. If you specify an expression, its result must be a number. In that case, the next action is determined as follows:
- If the expression evaluates to the priority of a policy with a lower priority (larger priority number) than the current policy, that policy is evaluated next.
- If the expression evaluates to a priority of the current policy, policy with the next highest priority is evaluated. An UNDEF event is triggered if:
- The expression cannot be evaluated.
- The expression evaluates to a number that is smaller than the highest priority in the policy bank but is not same as any policy's priority.
- The expression evaluates to a number that is smaller than the current policy's priority.

invoke Invoke other policy labels. After evaluating the policies in the invoked policy label, the appliance continues to evaluate policies that are bound to the current policy label (the selected bind point).

labelType Type of policy label invocation.

Possible values: policylabel

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

Example

i) bind cs policylabel cs_lab lbvs_1 pol_cs 1 2

rm cs policylabel

Removes a content switching policy label.

Synopsis

rm cs policylabel <labelName>

Arguments

labelName Name of the label to be removed.

Example

rm cs policylabel trans_http_url

rename cs policylabel

Rename a content switching policy label.

Synopsis

rename cs policylabel <labelName>@ <newName>@

Arguments

labelName The name of the content switching policylabel.

newName The new name of the content switching policylabel.

Example

rename cs policylabel oldname newname

show cs policylabel

Displays all the content switching policy labels, or just the specified policy label.

Synopsis

show cs policylabel

Arguments

labelName Name of the content switching policy label to display.

Output

cspolicylabeltype Protocol supported by the policy label. All policies bound to the policy label must either match the specified protocol or be a subtype of that protocol. Available settings function as follows:

- HTTP - Supports policies that process HTTP traffic. Used to access unencrypted Web sites. (The default.)
- SSL - Supports policies that process HTTPS/SSL encrypted traffic. Used to access encrypted Web sites.
- TCP - Supports policies that process any type of TCP traffic, including HTTP.

- SSL_TCP - Supports policies that process SSL-encrypted TCP traffic, including SSL.
- UDP - Supports policies that process any type of UDP-based traffic, including DNS.
- DNS - Supports policies that process DNS traffic.
- ANY - Supports all types of policies except HTTP, SSL, and TCP.
- SIP_UDP - Supports policies that process UDP based Session Initiation Protocol (SIP) traffic. SIP initiates, manages, and terminates multimedia communications sessions, and has emerged as the standard for Internet telephony (VoIP).
- RTSP - Supports policies that process Real Time Streaming Protocol (RTSP) traffic. RTSP provides delivery of multimedia and other streaming data, such as audio, video, and other types of streamed media.
- RADIUS - Supports policies that process Remote Authentication Dial In User Service (RADIUS) traffic. RADIUS supports combined authentication, authorization, and auditing services for network management.
- MYSQL - Supports policies that process MYSQL traffic.
- MSSQL - Supports policies that process Microsoft SQL traffic.

stateflag numpol number of polices bound to label.

hits Number of times policy label was invoked.

policyName Name of the content switching policy.

priority Specifies the priority of the policy.

targetVserver Name of the virtual server to which to forward requests that match the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

invoke devno count

Example

i) show cs policylabel cs_lab ii) show cs policylabel

unbind cs policylabel

Unbinds a content switching policy from a content switching policy label.

Synopsis

unbind cs policylabel <labelName> <policyName>

Arguments

labelName Name of the policy label from which to unbind a content switching policy.

policyName Name of the content switching policy to unbind from the label.

Example

unbind cs policylabel cs_lab pol_cs

add cs policylabel

Adds a content switching policy label.

Synopsis

add cs policylabel <labelName> <cspolicylabeltype>

Arguments

labelName Name for the policy label. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. The label name must be unique within the list of policy labels for content switching. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policylabel" or 'my policylabel').

cspolicylabeltype Protocol supported by the policy label. All policies bound to the policy label must either match the specified protocol or be a subtype of that protocol. Available settings function as follows:

- HTTP - Supports policies that process HTTP traffic. Used to access unencrypted Web sites. (The default.)
- SSL - Supports policies that process HTTPS/SSL encrypted traffic. Used to access encrypted Web sites.
- TCP - Supports policies that process any type of TCP traffic, including HTTP.

- SSL_TCP - Supports policies that process SSL-encrypted TCP traffic, including SSL.
- UDP - Supports policies that process any type of UDP-based traffic, including DNS.
- DNS - Supports policies that process DNS traffic.
- ANY - Supports all types of policies except HTTP, SSL, and TCP.
- SIP_UDP - Supports policies that process UDP based Session Initiation Protocol (SIP) traffic. SIP initiates, manages, and terminates multimedia communications sessions, and has emerged as the standard for Internet telephony (VoIP).
- RTSP - Supports policies that process Real Time Streaming Protocol (RTSP) traffic. RTSP provides delivery of multimedia and other streaming data, such as audio, video, and other types of streamed media.
- RADIUS - Supports policies that process Remote Authentication Dial In User Service (RADIUS) traffic. RADIUS supports combined authentication, authorization, and auditing services for network management.
- MYSQL - Supports policies that process MYSQL traffic.
- MSSQL - Supports policies that process Microsoft SQL traffic.

Possible values: HTTP, TCP, RTSP, SSL, SSL_TCP, UDP, DNS, SIP_UDP, SIP_TCP, ANY, RADIUS, RDP, MYSQL, MSSQL, ORACLE, DIAMETER, SSL_DIAMETER, FTP, DNS_TCP, SMPP, MQTT, MQTT_TLS, HTTP_QUIC

Example

add cs policylabel trans_http_url HTTP

cs-vserver

The following operations can be performed on "cs-vserver":

bind| rename| disable| add| set| enable| stat| unset| show| unbind| rm|

bind cs vserver

Binds a content switching virtual server to a content switching policy.

Synopsis

bind cs vserver <name> (-lbvserver <string> | -vServer <string> | (-policyName <string>) | (-domainName <string>) | -analyticsProfile <string>@)

Arguments

name Name of the content switching virtual server to which the content switching policy applies.

lbvserver Name of the default Load Balancing vserver bound. If for a particular content none of the Content Switching policies is evaluated to TRUE, that traffic is switched to default Load Balancing vserver. . Example: bind cs vserver cs1 -lbvserver lb1 Note: Use this parameter for default binding only.

vServer Name of the default gslb or vpn vserver bound to CS vserver of type GSLB/VPN. For Example: bind cs vserver cs1 -vserver gslb1 or bind cs vserver cs1 -vserver vpn1

policyName Name of the content switching policy to bind to the content switching virtual server Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after a policy is created. To bind a content switching policy, you need a content-based virtual server (content switching virtual server) and an address-based virtual server (load balancing virtual server). You can assign multiple policies to the virtual server pair. Note: When binding a CS virtual server to a default LB virtual server, the Policy Name parameter is optional. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

targetLBVserver Name of the Load Balancing virtual server to which the content is switched, if policy rule is evaluated to be TRUE. Example: bind cs vs cs1 -policyname pol1 -priority 101 -targetLBVserver lb1 Note: Use this parameter only in case of Content Switching policy bind operations to a CS vserver

priority Unsigned integer that determines the priority of the policy relative to other policies in this policy label (bound to the same bind point). A lower number specifies a higher priority. The maximum value of priority is 2147483647. Minimum value: 0

gotoPriorityExpression Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.

- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

type Bind point at which policy needs to be bound. Note: Content switching policies are evaluated only at request time.

Possible values: REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ

invoke Invoke a policy label if this policy's rule evaluates to TRUE.

labelType Type of label to be invoked.

Possible values: reqvserver, resvserver, policylabel

labelName Name of the label to be invoked.

domainName Domain name for which to change the time to live (TTL) and/or backup service IP address.

TTL backupIP cookieDomain cookieTimeout sitedomainTTL analyticsProfile bind cs vserver <vserver_name> -analyticsProfile <analytics-profile-name>.

Example

i) bind cs vserver csw-vip1 -policyname csw-policy1 -priority 13 ii) bind cs vserver csw-vip2 -policyname csw-ape-policy2 -priority 14 -gotoPriorityExpression NEXT iii) bind cs vserver csw-vip3 -policyname rewrite-policy1 -priority 17 -gotoPriorityExpression 'HTTP.REQ.HEADER("a").COUNT' -flowtype REQUEST -invoke policylabel label1

Related Commands

- show cs policy

rename cs vserver

Renames a content switching virtual server.

Synopsis

rename cs vserver <name>@ <newName>@

Arguments

name Existing name of the content switching virtual server.

newName New name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my name" or 'my name').

Example

rename cs vserver cs1 cs2

disable cs vserver

Disables a content switching virtual server.

Synopsis

disable cs vserver <name>@

Arguments

name Name of the virtual server to be disabled.

Example

disable vserver cs_vip

add cs vserver

Creates a content switching virtual server.

Synopsis

add cs vserver <name> <serviceType> ((<IPAddress> <port>) | -targetType GSLB | (-IPPattern <ippat> -IPMask <ipmask>)) [-insertVserverIPPort <insertVserverIPPort>] [-Listenpolicy <expression>] [-probeProtocol (TCP | HTTP)] [-redirectFromPort <port|*>]

Arguments

name Name for the content switching virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after the CS virtual server is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, my server or my server).

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

serviceType Protocol used by the virtual server.

Possible values: HTTP, SSL, TCP, FTP, RTSP, SSL_TCP, UDP, DNS, SIP_UDP, SIP_TCP, SIP_SSL, ANY, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, DNS_TCP, ORACLE, SMPP, PROXY, MONGO, MONGO_TLS, MQTT, MQTT_TLS, HTTP_QUIC

IPAddress IP address of the content switching virtual server.

targetType Virtual server target type.

Possible values: GSLB Default value: VAL_NOT_SET

dnsRecordType persistenceId IPPattern IP address pattern, in dotted decimal notation, for identifying packets to be accepted by the virtual server. The IP Mask parameter specifies which part of the destination IP address is matched against the pattern. Mutually exclusive with the IP Address parameter. For example, if the IP pattern assigned to the virtual server is 198.51.100.0 and the IP mask is 255.255.240.0 (a forward mask), the first 20 bits in the destination IP addresses

are matched with the first 20 bits in the pattern. The virtual server accepts requests with IP addresses that range from 198.51.96.1 to 198.51.111.254. You can also use a pattern such as 0.0.2.2 and a mask such as 0.0.255.255 (a reverse mask). If a destination IP address matches more than one IP pattern, the pattern with the longest match is selected, and the associated virtual server processes the request. For example, if the virtual servers, vs1 and vs2, have the same IP pattern, 0.0.100.128, but different IP masks of 0.0.255.255 and 0.0.224.255, a destination IP address of 198.51.100.128 has the longest match with the IP pattern of vs1. If a destination IP address matches two or more virtual servers to the same extent, the request is processed by the virtual server whose port number matches the port number in the request.

IPMask IP mask, in dotted decimal notation, for the IP Pattern parameter. Can have leading or trailing non-zero octets (for example, 255.255.240.0 or 0.0.255.255). Accordingly, the mask specifies whether the first n bits or the last n bits of the destination IP address in a client request are to be matched with the corresponding bits in the IP pattern. The former is called a forward mask. The latter is called a reverse mask.

range Number of consecutive IP addresses, starting with the address specified by the IP Address parameter, to include in a range of addresses assigned to this virtual server. Default value: 1 Minimum value: 1 Maximum value: 254

port Port number for content switching virtual server. Minimum value: 1

ipset The list of IPv4/IPv6 addresses bound to ipset would form a part of listening service on the current cs vserver

state Initial state of the load balancing virtual server.

Possible values: ENABLED, DISABLED Default value: ENABLED

stateupdate Enable state updates for a specific content switching virtual server. By default, the Content Switching virtual server is always UP, regardless of the state of the Load Balancing virtual servers bound to it. This parameter interacts with the global setting as follows: Global Level | Vserver Level | Result ENABLED ENABLED ENABLED ENABLED DISABLED ENABLED DISABLED ENABLED ENABLED DISABLED DISABLED DISABLED If you want to enable state updates for only some content switching virtual servers, be sure to disable the state update parameter.

Possible values: ENABLED, DISABLED, UPDATEONBACKENDUPDATE Default value: DISABLED

cacheable Use this option to specify whether a virtual server, used for load balancing or content switching, routes requests to the cache redirection virtual server before sending it to the configured servers.

Possible values: YES, NO Default value: NO

redirectURL URL to which traffic is redirected if the virtual server becomes unavailable. The service type of the virtual server should be either HTTP or SSL. Caution: Make sure that the domain in the URL does not match the domain specified for a content switching policy. If it does, requests are continuously redirected to the unavailable virtual server.

cltTimeout Idle time, in seconds, after which the client connection is terminated. The default values are: 180 seconds for HTTP/SSL-based services. 9000 seconds for other TCP-based services. 120 seconds for DNS-based services. 120 seconds for other UDP-based services. Default value: -1 Maximum value: 31536000

soMethod Type of spillover used to divert traffic to the backup virtual server when the primary virtual server reaches the spillover threshold. Connection spillover is based on the number of connections. Bandwidth spillover is based on the total Kbps of incoming and outgoing traffic.

Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence Maintain source-IP based persistence on primary and backup virtual servers.

Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeOut Time-out value, in minutes, for spillover persistence. Default value: 2 Minimum value: 2 Maximum value: 1440

soThreshold Depending on the spillover method, the maximum number of connections or the maximum total bandwidth (Kbps) that a virtual server can handle before spillover occurs. Minimum value: 1 Maximum value: 4294967287

soBackupAction Action to be performed if spillover is to take effect, but no backup chain to spillover is usable or exists

Possible values: DROP, ACCEPT, REDIRECT

redirectPortRewrite State of port rewrite while performing HTTP redirect.

Possible values: ENABLED, DISABLED Default value: DISABLED

downStateFlush Flush all active transactions associated with a virtual server whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions.

Possible values: ENABLED, DISABLED Default value: ENABLED

backupVServer Name of the backup virtual server that you are configuring. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the backup virtual server is created. You can assign a different backup virtual server or rename the existing virtual server. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks.

disablePrimaryOnDown Continue forwarding the traffic to backup virtual server even after the primary server comes UP from the DOWN state.

Possible values: ENABLED, DISABLED Default value: DISABLED

insertVserverIPPort Insert the virtual server's VIP address and port number in the request header. Available values function as follows: VIPADDR - Header contains the vserver's IP address and port number without any translation. OFF - The virtual IP and port header insertion option is disabled. V6TOV4MAPPING - Header contains the mapped IPv4 address corresponding to the IPv6 address of the vserver and the port number. An IPv6 address can be mapped to a user-specified IPv4 address using the set ns ip6 command.

Possible values: OFF, VIPADDR, V6TOV4MAPPING

vipHeader Name of virtual server IP and port header, for use with the VServer IP Port Insertion parameter.

rtspNat Enable network address translation (NAT) for real-time streaming protocol (RTSP) connections.

Possible values: ON, OFF Default value: OFF

AuthenticationHost FQDN of the authentication virtual server. The service type of the virtual server should be either HTTP or SSL.

Authentication Authenticate users who request a connection to the content switching virtual server.

Possible values: ON, OFF Default value: OFF

Listenpolicy String specifying the listen policy for the content switching virtual server. Can be either the name of an existing expression or an in-line expression. Default value: "NONE"

Listenpriority Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server the virtual server whose listen policy has the highest priority (the lowest priority number) accepts the request. Default value: 101 Minimum value: 0 Maximum value: 100

authn401 Enable HTTP 401-response based authentication.

Possible values: ON, OFF Default value: OFF

authnVsName Name of authentication virtual server that authenticates the incoming user requests to this content switching virtual server.

push Process traffic with the push virtual server that is bound to this content switching virtual server (specified by the Push VServer parameter). The service type of the push virtual server should be either HTTP or SSL.

Possible values: ENABLED, DISABLED Default value: DISABLED

pushVserver Name of the load balancing virtual server, of type PUSH or SSL_PUSH, to which the server pushes updates received on the client-facing load balancing virtual server.

pushLabel Expression for extracting the label from the response received from server. This string can be either an existing rule name or an inline expression. The service type of the virtual server should be either HTTP or SSL. Default value: "none"

pushMultiClients Allow multiple Web 2.0 connections from the same client to connect to the virtual server and expect updates.

Possible values: YES, NO Default value: NO

tcpProfileName Name of the TCP profile containing TCP configuration settings for the virtual server.

httpProfileName Name of the HTTP profile containing HTTP configuration settings for the virtual server. The service type of the virtual server should be either HTTP or SSL.

dbProfileName Name of the DB profile.

oracleServerVersion Oracle server version

Possible values: 10G, 11G Default value: 10G

comment Information about this virtual server.

mssqlServerVersion The version of the MSSQL server

Possible values: 70, 2000, 2000SP1, 2005, 2008, 2008R2, 2012, 2014 Default value: 2008R2

l2Conn Use L2 Parameters to identify a connection

Possible values: ON, OFF

mysqlProtocolVersion The protocol version returned by the mysql vserver. Default value: 10 Minimum value: 0

mysqlServerVersion The server version string returned by the mysql vserver. Default value: NSA_MYSQL_SERVER_VER_DEFAULT

mysqlCharacterSet The character set returned by the mysql vserver. Default value: 8 Minimum value: 0

mysqlServerCapabilities The server capabilities returned by the mysql vserver. Default value: 41613 Minimum value: 0

appflowLog Enable logging appflow flow information

Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile The name of the network profile.

icmpVsrResponse Can be active or passive

Possible values: PASSIVE, ACTIVE Default value: PASSIVE

RHIstate A host route is injected according to the setting on the virtual servers

- If set to PASSIVE on all the virtual servers that share the IP address, the appliance always injects the hostroute.
- If set to ACTIVE on all the virtual servers that share the IP address, the appliance injects even if one virtual server is UP.
- If set to ACTIVE on some virtual servers and PASSIVE on the others, the appliance, injects even if one virtual server set to ACTIVE is UP.

Possible values: PASSIVE, ACTIVE Default value: PASSIVE

authnProfile Name of the authentication profile to be used when authentication is turned on.

dnsProfileName Name of the DNS profile to be associated with the VServer. DNS profile properties will applied to the transactions processed by a VServer. This parameter is valid only for DNS and DNS-TCP VServers.

dtls This option starts/stops the dtls service on the vserver

Possible values: ON, OFF Default value: OFF

persistenceType Type of persistence for the virtual server. Available settings function as follows:

- SOURCEIP - Connections from the same client IP address belong to the same persistence session.
- COOKIEINSERT - Connections that have the same HTTP Cookie, inserted by a Set-Cookie directive from a server, belong to the same persistence session.
- SSLSESSION - Connections that have the same SSL Session ID belong to the same persistence session.

Possible values: SOURCEIP, COOKIEINSERT, SSLSESSION, NONE

persistMask Persistence mask for IP based persistence types, for IPv4 virtual servers. Default value: 0xFFFFFFFF

v6persistmasklen Persistence mask for IP based persistence types, for IPv6 virtual servers. Default value: 128 Minimum value: 1 Maximum value: 128

timeout Time period for which a persistence session is in effect. Default value: 2 Maximum value: 1440

cookieName Use this parameter to specify the cookie name for COOKIE peristence type. It specifies the name of cookie with a maximum of 32 characters. If not specified, cookie name is internally generated.

persistenceBackup Backup persistence type for the virtual server. Becomes operational if the primary persistence mechanism fails.

Possible values: SOURCEIP, NONE

backupPersistenceTimeout Time period for which backup persistence is in effect. Default value: 2 Minimum value: 2 Maximum value: 1440

probeProtocol Citrix ADC provides support for external health check of the vserver status. Select HTTP or TCP probes for healthcheck

Possible values: TCP, HTTP

probeSuccessResponseCode HTTP code to return in SUCCESS case. Default value: "200 OK"

probePort Citrix ADC provides support for external health check of the vserver status. Select port for HTTP/TCP monitring Default value: 0

quicProfileName Name of QUIC profile which will be attached to the Content Switching VServer.

redirectFromPort Port number for the virtual server, from which we absorb the traffic for http redirect Minimum value: 1

httpsRedirectUrl URL to which all HTTP traffic received on the port specified in the -redirectFromPort parameter is redirected.

Example

1. You can use precedence when certain client attributes (e.g., browser type) require to be served with different content. All other clients can then be served from content distributed among the servers. If the precedence is configured as URL, the incoming request URL is evaluated against the content switching policies created with the -url argument. If none of the policies match, the request is applied against the content any switching policies created with the -rule argument.
2. Precedence can also be used when certain content (such as images) is the same for all clients, but other content (such as text) is different for different clients. In this case, the images will be served to all clients, but the text will be served to specific clients based on attributes such as Accept-Language.

Related Commands

- add cs policy

set cs vserver

Modifies the configuration of a content switching virtual server.

Synopsis

set cs vserver <name> [-insertVserverIPPort <insertVserverIPPort>] [-domainName <string>] [-probeProtocol (TCP | HTTP)]

Arguments

name Identifies the virtual server name (created with the add cs vserver command).

IPAddress The new IP address of the virtual server.

ipset The list of IPv4/IPv6 addresses bound to ipset would form a part of listening service on the current cs vserver

IPPattern IP address pattern, in dotted decimal notation, for identifying packets to be accepted by the virtual server. The IP Mask parameter specifies which part of the destination IP address is matched against the pattern. Mutually exclusive with the IP Address parameter. For example, if the IP pattern assigned to the virtual server is 198.51.100.0 and the IP mask is 255.255.240.0 (a forward mask), the first 20 bits in the destination IP addresses are matched with the first 20 bits in the pattern. The virtual server accepts requests with IP addresses that range from 198.51.96.1 to 198.51.111.254. You can also use a pattern such as 0.0.2.2 and a mask such as 0.0.255.255 (a reverse mask). If a destination IP address matches more than one IP pattern, the pattern with the longest match is selected, and the associated virtual server processes the request. For example, if the virtual servers, vs1 and vs2, have the same IP pattern, 0.0.100.128, but different IP masks of 0.0.255.255 and 0.0.224.255, a destination IP address of 198.51.100.128 has the longest match with the IP pattern of vs1. If a destination IP address matches two or more virtual servers to the same extent, the request is processed by the virtual server whose port number matches the port number in the request.

IPMask IP mask, in dotted decimal notation, for the IP Pattern parameter. Can have leading or trailing non-zero octets (for example, 255.255.240.0 or 0.0.255.255). Accordingly, the mask specifies whether the first n bits or the last n bits of the destination IP address in a client request are to be matched with the corresponding bits in the IP pattern. The former is called a forward mask. The latter is called a reverse mask.

stateupdate Enable state updates for a specific content switching virtual server. By default, the Content Switching virtual server is always UP, regardless of the state of the Load Balancing virtual servers bound to it. This parameter interacts with the global setting as follows: Global Level | Vserver Level | Result ENABLED ENABLED ENABLED ENABLED DISABLED ENABLED DISABLED ENABLED ENABLED DISABLED DISABLED DISABLED If you want to enable state updates for only some content switching virtual servers, be sure to disable the state update parameter.

Possible values: ENABLED, DISABLED, UPDATEONBACKENDUPDATE Default value: DISABLED

backupVServer Name of the backup virtual server that you are configuring. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the backup virtual server is created. You can assign a different backup virtual server or rename the existing virtual server. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks.

redirectURL The redirect URL for content switching.

cacheable The option to specify whether a virtual server used for content switching will route requests to the cache redirection virtual server before sending it to the configured servers.

Possible values: YES, NO Default value: NO

cltTimeout Client timeout in seconds. Default value: -1 Maximum value: 31536000

soMethod The spillover factor. When traffic on the main virtual server reaches this threshold, additional traffic is sent to the backupvserver.

Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence Maintain source-IP based persistence on primary and backup virtual servers.

Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeOut The spillover persistency entry timeout. Default value: 2 Minimum value: 2 Maximum value: 1440

soThreshold Depending on the spillover method, the maximum number of connections or the maximum total bandwidth (Kbps) that a virtual server can handle before spillover occurs. Minimum value: 1 Maximum value: 4294967287

soBackupAction Action to be performed if spillover is to take effect, but no backup chain to spillover is usable or exists

Possible values: DROP, ACCEPT, REDIRECT

redirectPortRewrite SSL redirect port rewrite.

Possible values: ENABLED, DISABLED Default value: DISABLED

downStateFlush Flush all active transactions associated with a virtual server whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions.

Possible values: ENABLED, DISABLED Default value: ENABLED

disablePrimaryOnDown Continue forwarding the traffic to backup virtual server even after the primary server comes UP from the DOWN state.

Possible values: ENABLED, DISABLED Default value: DISABLED

insertVserverIPPort The virtual IP and port header insertion option for the vserver.

- VIPADDR - Header contains the vserver's IP address and port number without any translation.
- OFF - The virtual IP and port header insertion option is disabled.
- V6TOV4MAPPING - Header contains the mapped IPv4 address that corresponds to the IPv6 address of the vserver and the port number. An IPv6 address can be mapped to a user-specified IPv4 address using the set ns ip6 command.

Possible values: OFF, VIPADDR, V6TOV4MAPPING

vipHeader The name of virtual IP and port header.

rtspNat Enable network address translation (NAT) for real-time streaming protocol (RTSP) connections.

Possible values: ON, OFF Default value: OFF

AuthenticationHost FQDN of the authentication virtual server. The service type of the virtual server should be either HTTP or SSL.

Authentication Authenticate users who request a connection to the content switching virtual server.

Possible values: ON, OFF Default value: OFF

Listenpolicy String specifying the listen policy for the content switching virtual server. Can be either the name of an existing expression or an in-line expression. Default value: "NONE"

Listenpriority Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server the virtual server

whose listen policy has the highest priority (the lowest priority number) accepts the request. Default value: 101 Minimum value: 0 Maximum value: 100

authn401 Enable HTTP 401-response based authentication.

Possible values: ON, OFF Default value: OFF

authnVsName Name of authentication virtual server that authenticates the incoming user requests to this content switching virtual server.

push Process traffic with the push virtual server that is bound to this content switching virtual server (specified by the Push VServer parameter). The service type of the push virtual server should be either HTTP or SSL.

Possible values: ENABLED, DISABLED Default value: DISABLED

pushVserver Name of the load balancing virtual server, of type PUSH or SSL_PUSH, to which the server pushes updates received on the client-facing load balancing virtual server.

pushLabel Expression for extracting the label from the response received from server. This string can be either an existing rule name or an inline expression. The service type of the virtual server should be either HTTP or SSL. Default value: "none"

pushMultiClients Allow multiple Web 2.0 connections from the same client to connect to the virtual server and expect updates.

Possible values: YES, NO Default value: NO

tcpProfileName Name of the TCP profile containing TCP configuration settings for the virtual server.

httpProfileName Name of the HTTP profile containing HTTP configuration settings for the virtual server. The service type of the virtual server should be either HTTP or SSL.

dbProfileName Name of the DB profile.

comment Information about this virtual server.

l2Conn Use L2 Parameters to identify a connection

Possible values: ON, OFF

mssqlServerVersion The version of the MSSQL server

Possible values: 70, 2000, 2000SP1, 2005, 2008, 2008R2, 2012, 2014 Default value: 2008R2

mysqlProtocolVersion The protocol version returned by the mysql vserver. Default value: 10 Minimum value: 0

oracleServerVersion Oracle server version

Possible values: 10G, 11G Default value: 10G

mysqlServerVersion The server version string returned by the mysql vserver. Default value: NSA_MYSQL_SERVER_VER_DEFAULT

mysqlCharacterSet The character set returned by the mysql vserver. Default value: 8 Minimum value: 0

mysqlServerCapabilities The server capabilities returned by the mysql vserver. Default value: 41613 Minimum value: 0

appflowLog Enable logging appflow flow information

Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile The name of the network profile.

authnProfile Name of the authentication profile to be used when authentication is turned on.

icmpVsrResponse Can be active or passive

Possible values: PASSIVE, ACTIVE Default value: PASSIVE

RHIstate A host route is injected according to the setting on the virtual servers

- If set to PASSIVE on all the virtual servers that share the IP address, the appliance always injects the hostroute.
- If set to ACTIVE on all the virtual servers that share the IP address, the appliance injects even if one virtual server is UP.
- If set to ACTIVE on some virtual servers and PASSIVE on the others, the appliance, injects even if one virtual server set to ACTIVE is UP.

Possible values: PASSIVE, ACTIVE Default value: PASSIVE

dnsProfileName Name of the DNS profile to be associated with the VServer. DNS profile properties will applied to the transactions processed by a VServer. This parameter is valid only for DNS and DNS-TCP VServers.

dnsRecordType persistenceId domainName Domain name for which to change the time to live (TTL) and/or backup service IP address.

TTL backupIP cookieDomain cookieTimeout sitedomainTTL dtls This option starts/stops the dtls service on the vserver

Possible values: ON, OFF Default value: OFF

persistenceType Type of persistence for the virtual server. Available settings function as follows:

- SOURCEIP - Connections from the same client IP address belong to the same persistence session.
- COOKIEINSERT - Connections that have the same HTTP Cookie, inserted by a Set-Cookie directive from a server, belong to the same persistence session.
- SSLSESSION - Connections that have the same SSL Session ID belong to the same persistence session.

Possible values: SOURCEIP, COOKIEINSERT, SSLSESSION, NONE

persistMask Persistence mask for IP based persistence types, for IPv4 virtual servers. Default value: 0xFFFFFFFF

v6persistmasklen Persistence mask for IP based persistence types, for IPv6 virtual servers. Default value: 128 Minimum value: 1 Maximum value: 128

timeout Time period for which a persistence session is in effect. Default value: 2 Maximum value: 1440

cookieName Use this parameter to specify the cookie name for COOKIE peristence type. It specifies the name of cookie with a maximum of 32 characters. If not specified, cookie name is internally generated.

persistenceBackup Backup persistence type for the virtual server. Becomes operational if the primary persistence mechanism fails.

Possible values: SOURCEIP, NONE

backupPersistenceTimeout Time period for which backup persistence is in effect. Default value: 2 Minimum value: 2 Maximum value: 1440

probeProtocol Citrix ADC provides support for external health check of the vserver status. Select HTTP or TCP probes for healthcheck

Possible values: TCP, HTTP

probeSuccessResponseCode HTTP code to return in SUCCESS case. Default value: "200 OK"

probePort Citrix ADC provides support for external health check of the vserver status. Select port for HTTP/TCP monitring Default value: 0

quicProfileName Name of QUIC profile which will be attached to the Content Switching VServer.

redirectFromPort Port number for the virtual server, from which we absorb the traffic for http redirect Minimum value: 1

httpsRedirectUrl URL to which all HTTP traffic received on the port specified in the -redirectFromPort parameter is redirected.

Related Commands

- show cs policy

enable cs vserver

Enables a content switching virtual server.

Synopsis

enable cs vserver <name>@

Arguments

name Name of the content switching virtual server to enable. Note: Virtual servers, when added, are enabled by default.

Example

enable vserver cs_vip

stat cs vserver

Displays statistics of all content switching virtual servers, or statistics for just the specified content switching virtual server.

Synopsis

stat cs vserver

Arguments

name Name of the content switching virtual server for which to display statistics. To display statistics for all configured Content Switching virtual servers, do not specify a value for this parameter.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Average client TTLB (cltTTLB) Average TTLB between the client and the server. TTLB is the time interval between sending the request packet to a service and receiving the ACK for response from client.

Apdex for client response times. (cltResponseTimeApdex) Vserver APDEX index based on client response times.

Current Client Est connections (ClntEstConn) Number of client connections in ESTABLISHED state.

Number of Bytes processed by ADS Service Total IP payload sent and received

IP address (IP) The IP address on which the service is running.

Port (port) The port on which the service is running.

Vserver protocol (Protocol) Protocol associated with the vserver

State Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)

Vserver hits (Hits) Total vserver hits

Requests (Req) Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Responses (Rsp) Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Request bytes (Reqb) Total number of request bytes received on this service or virtual server.

Response bytes (Rspb) Number of response bytes received by this service or virtual server.

Total Packets rcvd (PktRx) Total number of packets received by this service or virtual server.

Total Packets sent (PktTx) Total number of packets sent.

Current client connections (ClntConn) Number of current client connections.

Current server connections (SvrConn) Number of current connections to the actual servers behind the virtual server.

Current Persistence Sessions (PersistenceSessions) current vserver owned persistence sessions

Current Backup Persistence Sessions (BackupPersistenceSessions) current vserver owned backup persistence sessions

Spill Over Threshold (SOThresh) Spill Over Threshold set on the VServer.

Spill Over Hits (NumSo) Number of times vserver experienced spill over.

Labeled Connection (LblConn) Number of Labeled connection on this vserver

Push Labeled Connection (PushLbl) Number of labels for this push vserver.

Deferred Request (DefReq) Number of deferred request on this vserver

Invalid Request/Response (InvldReqRsp) Number invalid requests/responses on this vserver

Invalid Request/Response Dropped (InvldReqRspDrp) Number invalid requests/responses dropped on this vserver

Vserver Down Backup Hits (VserverDownBackupHits) Number of times traffic was diverted to backup vserver since primary vserver was DOWN.

Current Multipath TCP sessions (MptcpSess) Current Multipath TCP sessions

Current Multipath TCP subflows (subflowConn) Current Multipath TCP subflows

No of http max header size packet parsing failures (httpMaxHdrSzPkts) Number of http max header size packet parsing failures

Number of HTTP requests exceeding max header field length (httpMaxHdrFldLenPkts) Number of HTTP requests exceeding max header field length

max ooo packets threshold hits (tcpMaxoooPkts) No of times max out of order packets reached

Total transactions for Client TTLB (totCltTTLBTransactions) Total transactions where client TTLB is calculated.

Tolerating TTLB Transactions (toleratingTTLBTransactions) Tolerable transactions based on APDEX threshold (>T && <4T).

Frustrating TTLB Transactions (frustratingTTLBTransactions) Frustrating transactions based on APDEX threshold (>4T).

Current Server Est connections (SvrEstConn) Number of server connections in ESTABLISHED state.

unset cs vserver

Unset the parameters of a content switching virtual server..Refer to the set cs vserver command for meanings of the arguments.

Synopsis

unset cs vserver <name>

Related Commands

- show cs policy

show cs vserver

Displays all existing content switching virtual servers, or just the specified virtual server.

Synopsis

show cs vserver show cs vserver stats - alias for 'stat cs vserver'

Arguments

name Name of a content switching virtual server for which to display information, including the policies bound to the virtual server. To display a list of all configured Content Switching virtual servers, do not specify a value for this parameter.

Output

insertVserverIPPort The virtual IP and port header insertion option for the vserver.

vipHeader The name of virtual IP and port header.

IPAddress The IP address of the virtual server.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

IPAddress IP address of the content switching virtual server.

IPPattern The IP address of the virtual server.

IPMask The IP address mask of the virtual server.

stateflag value The ssl card status for the transparent ssl cs vserver.

port Port number for content switching virtual server.

ipset The list of IPv4/IPv6 addresses bound to ipset would form a part of listening service on the current cs vserver

range Number of consecutive IP addresses, starting with the address specified by the IP Address parameter, to include in a range of addresses assigned to this virtual server.

serviceType Protocol used by the virtual server.

ngname Nodegroup devno to which this csvserver belongs to

type Virtual server type.

vsvrcfgflags Contains the config info of vserver to be used at validation

state The state of the cs vserver.

stateupdate Enable state updates for a specific content switching virtual server. By default, the Content Switching virtual server is always UP, regardless of the state of the Load Balancing virtual servers bound to it. This parameter interacts with the global setting as follows: Global Level | Vserver Level | Result ENABLED ENABLED ENABLED ENABLED DISABLED ENABLED DISABLED ENABLED ENABLED DISABLED DISABLED DISABLED If you want to enable state updates for only some content switching virtual servers, be sure to disable the state update parameter.

status Status.

cacheType Cache type.

redirect Redirect URL string.

precedence Type of precedence to use for both RULE-based and URL-based policies on the content switching virtual server. With the default (RULE) setting, incoming requests are evaluated against the rule-based content switching policies. If none of the rules match, the URL in the request is evaluated against the URL-based content switching policies.

redirectURL The redirect URL for content switching.

Authentication Authentication.

authn401 HTTP 401 response based authentication.

authnVsName Name of authentication virtual server that authenticates the incoming user requests to this content switching virtual server.

caseSensitive Consider case in URLs (for policies that use URLs instead of RULES). For example, with the ON setting, the URLs /a/1.html and /A/1.HTML are treated differently and can have different targets (set by content switching policies). With the OFF setting, /a/1.html and /A/1.HTML are switched to the same target.

homePage Home page.

dnsVserverName DNS vserver name.

domain Domain.

rule Rule.

policyName Policies bound to this vserver.

hits Number of hits.

piPolicyhits Number of hits.

serviceName Service name.

weight Weight for this service.

cacheVserver Cache vserver name.

targetVserver target vserver name.

backupVServer Name of the backup virtual server that you are configuring. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the backup virtual server is created. You can assign a different backup virtual server or rename the existing virtual server. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks.

priority Priority for the policy.

cltTimeout Idle time, in seconds, after which the client connection is terminated. The default values are: 180 seconds for HTTP/SSL-based services. 9000 seconds for other TCP-based services. 120 seconds for DNS-based services. 120 seconds for other UDP-based services.

Listenpolicy The string is listenpolicy configured for lb vserver

Listenpriority This parameter is the priority for listen policy of LB Vserver.

soMethod Type of spillover used to divert traffic to the backup virtual server when the primary virtual server reaches the spillover threshold. Connection spillover is based on the number of connections. Bandwidth spillover is based on the total Kbps of incoming and outgoing traffic.

soPersistence Maintain source-IP based persistence on primary and backup virtual servers.

soPersistenceTimeOut Time-out value, in minutes, for spillover persistence.

soThreshold Depending on the spillover method, the maximum number of connections or the maximum total bandwidth (Kbps) that a virtual server can handle before spillover occurs.

soBackupAction Action to be performed if spillover is to take effect, but no backup chain to spillover is usable or exists

cacheable The state of caching.

url URL string.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

redirectPortRewrite Redirect port rewrite.

downStateFlush Flush all active transactions associated with a virtual server whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions.

disablePrimaryOnDown Tells whether traffic will continue reaching backup vservers even after primary comes UP from DOWN state.

type The bindpoint to which the policy is bound

invoke Invoke flag.

labelType The invocation type.

labelName Name of the label invoked.

gt2GB This argument has no effect.

stateChangeTimeSec Time when last state change happened. Seconds part.

stateChangeTimemSec Time at which last state change happened. Milliseconds part.

ticksSinceLastStateChange Time in 10 millisecond ticks since the last state change.

rtspNat Enable network address translation (NAT) for real-time streaming protocol (RTSP) connections.

AuthenticationHost FQDN of the authentication virtual server. The service type of the virtual server should be either HTTP or SSL.

push Process traffic with the push virtual server that is bound to this content switching virtual server (specified by the Push VServer parameter). The service type of the push virtual server should be either HTTP or SSL.

pushVserver Name of the load balancing virtual server, of type PUSH or SSL_PUSH, to which the server pushes updates received on the client-facing load balancing virtual server.

pushLabel Expression for extracting the label from the response received from server. This string can be either an existing rule name or an inline expression. The service type of the virtual server should be either HTTP or SSL.

pushMultiClients Allow multiple Web 2.0 connections from the same client to connect to the virtual server and expect updates.

tcpProfileName Name of the TCP profile containing TCP configuration settings for the virtual server.

httpProfileName Name of the HTTP profile containing HTTP configuration settings for the virtual server. The service type of the virtual server should be either HTTP or SSL.

dbProfileName Name of the DB profile.

comment Information about this virtual server.

appfwPolicyFlag flags policySubType oracleServerVersion Oracle server version

mssqlServerVersion The version of the MSSQL server

l2Conn Use L2 Parameters to identify a connection

ruleType Rule type.

mysqlProtocolVersion The protocol version returned by the mysql vserver.

mysqlServerVersion The server version string returned by the mysql vserver.

mysqlCharacterSet The character set returned by the mysql vserver.

mysqlServerCapabilities The server capabilities returned by the mysql vserver.

appflowLog Enable logging appflow flow information

netProfile The name of the network profile.

state Initial state of the load balancing virtual server.

icmpVsrResponse Can be active or passive

RHIstate A host route is injected according to the setting on the virtual servers

- If set to PASSIVE on all the virtual servers that share the IP address, the appliance always injects the hostroute.

- If set to ACTIVE on all the virtual servers that share the IP address, the appliance injects even if one virtual server is UP.
- If set to ACTIVE on some virtual servers and PASSIVE on the others, the appliance, injects even if one virtual server set to ACTIVE is UP.

lbvserver Name of the default lb vserver bound. Use this param for Default binding only. For Example: bind cs vserver cs1 -lbvserver lb1

vServer Name of the default gslb or vpn vserver bound to CS vserver of type GSLB/VPN. For Example: bind cs vserver cs1 -vserver gslb1 or bind cs vserver cs1 -vserver vpn1

targetLBVserver target vserver name.

contentVsvrFlag authnProfile Name of the authentication profile to be used when authentication is turned on.

dnsProfileName Name of the DNS profile to be associated with the VServer. DNS profile properties will applied to the transactions processed by a VServer. This parameter is valid only for DNS and DNS-TCP VServers.

targetType Virtual server target type.

domainName Domain name for which to change the time to live (TTL) and/or backup service IP address.

TTL backupIP cookieDomain cookieTimeout sitedomainTTL dnsRecordType persistenceId analyticsProfile Name of the analytics profile bound to the LB vserver.

dtls This option starts/stops the dtls service on the vserver

noDefaultBindings to determine if the configuration will have default ssl CIPHER and ECC curve bindings

persistenceType Type of persistence for the virtual server. Available settings function as follows:

- SOURCEIP - Connections from the same client IP address belong to the same persistence session.
- COOKIEINSERT - Connections that have the same HTTP Cookie, inserted by a Set-Cookie directive from a server, belong to the same persistence session.
- SSLSESSION - Connections that have the same SSL Session ID belong to the same persistence session.

persistMask Persistence mask for IP based persistence types, for IPv4 virtual servers.

v6persistmasklen Persistence mask for IP based persistence types, for IPv6 virtual servers.

timeout Time period for which a persistence session is in effect.

cookieName Use this parameter to specify the cookie name for COOKIE peristence type. It specifies the name of cookie with a maximum of 32 characters. If not specified, cookie name is internally generated.

version Cookie version

vserverId Vserver Id of vserver

cookieIpPort Vserver id of the lb vserver that is inserted into the set-cookie HTTP header

persistenceBackup Backup persistence type for the virtual server. Becomes operational if the primary persistence mechanism fails.

backupPersistenceTimeout Time period for which backup persistence is in effect.

tcpProbePort Port number for external TCP probe. NetScaler provides support for external TCP health check of the vserver status over the selected port. This option is only supported for vservers assigned with an IPAddress or ipset.

probeProtocol Citrix ADC provides support for external health check of the vserver status. Select HTTP or TCP probes for healthcheck

probePort Citrix ADC provides support for external health check of the vserver status. Select port for HTTP/TCP monitring

probeSuccessResponseCode HTTP code to return in SUCCESS case.

quicProfileName Name of QUIC profile which will be attached to the Content Switching VServer.

redirectFromPort Port number for the virtual server, from which we absorb the traffic for http redirect

httpsRedirectUrl URL to which all HTTP traffic received on the port specified in the -redirectFromPort parameter is redirected.

devno count

Related Commands

- show cs policy

unbind cs vserver

Unbinds the virtual server from the content switching policy.

Synopsis

unbind cs vserver <name> (-vServer <string> | (-policyName <string>) | -domainName <string> | -lbvserver <string> | -analyticsProfile <string>@)

Arguments

name Name of the virtual server to unbind from the policy.

vServer Name of the default gslb or vpn vserver bound to CS vserver of type GSLB/VPN. For Example: bind cs vserver cs1 -vserver gslb1 or bind cs vserver cs1 -vserver vpn1

policyName Name of the policy from which to unbind the content switching virtual server. Note: To unbind the content switching virtual server from the default policy, do not specify a value for this parameter.

type For rewrite policies, the traffic flow to which the policy applies. Note: This parameter applies only to rewrite policies, because content switching policies are evaluated only at request time.

Possible values: REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ

priority Priority number of the policy from which to unbind the content switching virtual server. Minimum value: 1

domainName Domain name for which to change the time to live (TTL) and/or backup service IP address.

lbvserver Name of the default lb vserver bound. Use this param for Default binding only. For Example: bind cs vserver cs1 -lbvserver lb1 Default value: "default_lb"

analyticsProfile unbind cs vserver <vserver_name> -analyticsProfile <analytics-profile-name>.

rm cs vserver

Removes a content switching virtual server.

Synopsis

rm cs vserver <name>@ ...

Arguments

name Name of the virtual server to be removed.

Example

rm vserver cs_vip

db

Db

The entities on which you can perform NetScaler CLI operations:

- db-dbProfile
- db-user

db-dbProfile

The following operations can be performed on "db-dbProfile":

rm| set| show| unset| add|

rm db dbProfile

Remove a DB profile on the Citrix ADC

Synopsis

rm db dbProfile <name>

Arguments

name Name of the DB profile

Example

rm dbprofile <profile name>

set db dbProfile

Set/modify DB profile values

Synopsis

set db dbProfile <name>

Arguments

name Name for the database profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after the profile is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

interpretQuery If ENABLED, inspect the query and update the connection information, if required. If DISABLED, forward the query to the server.

Possible values: YES, NO Default value: YES

stickiness If the queries are related to each other, forward to the same backend server.

Possible values: YES, NO Default value: NO

kcdAccount Name of the KCD account that is used for Windows authentication.

conMultiplex Use the same server-side connection for multiple client-side requests. Default is enabled.

Possible values: ENABLED, DISABLED Default value: ENABLED

enableCachingConMuxOFF Enable caching when connection multiplexing is OFF.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set dbprofile <profile name> -interpretQuery YES -stickyness YES

show db dbProfile

Display all the configured DB profiles in the system. If a name is specified, then only that profile is shown.

Synopsis

show db dbProfile

Arguments

name Name of the DB profile.

Output

interpretQuery Interpret Queries on NS

stickiness Stickyness for Queries

kcdAccount KCD account for windows authentication

conMultiplex Enable/Disable Connection Multiplexing

refCnt Profile Reference Count

enableCachingConMuxOFF Enable Caching When Connection Multiplexing is OFF

stateflag State flag

devno count

Example

show dbprofile

unset db dbProfile

Unset DB profile values.Refer to the set db dbProfile command for meanings of the arguments.

Synopsis

unset db dbProfile <name>

add db dbProfile

Add a new DB profile on the Citrix ADC

Synopsis

add db dbProfile <name>

Arguments

name Name for the database profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after the profile is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

interpretQuery If ENABLED, inspect the query and update the connection information, if required. If DISABLED, forward the query to the server.

Possible values: YES, NO Default value: YES

stickiness If the queries are related to each other, forward to the same backend server.

Possible values: YES, NO Default value: NO

kcdAccount Name of the KCD account that is used for Windows authentication.

conMultiplex Use the same server-side connection for multiple client-side requests. Default is enabled.

Possible values: ENABLED, DISABLED Default value: ENABLED

enableCachingConMuxOFF Enable caching when connection multiplexing is OFF.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

add dbprofile <profile name> -interpretQuery YES -stickyness YES -kcdaccount account

db-user

The following operations can be performed on "db-user":

show| set| rm| add|

show db user

Displays the specified database user or, if no user is specified, all the database users configured on the appliance.

Synopsis

show db user

Arguments

userName Name of the database user.

loggedIn Display the names of all database users currently logged on to the Citrix ADC.

Output

password Password for logging on to the database. Must be the same as the password specified in the database.

devno count stateflag

set db user

Modifies the password of an existing database user.

Synopsis

set db user <userName>

Arguments

userName Name of the database user.

password The database users password. If you use the CLI, you are prompted for this password after specifying the user name.

Example

set db user johndoe The above command sets the password for johndoe to abcd (Password to be suplied on prompt)

rm db user

Removes a database user from the Citrix ADC. Requests from the user are no longer authenticated or routed to the database server.

Synopsis

rm db user <userName>

Arguments

userName Name of the database user to remove.

add db user

Adds a database user. The user name and password that you specify in this command are added to the nsconfig file and used to authenticate the user.

Synopsis

add db user <userName> {-password }

Arguments

userName Name of the database user. Must be the same as the user name specified in the database.

password Password for logging on to the database. Must be the same as the password specified in the database.

Example

add db user johndoe -password secret

dns

dns-aaaaRec

The following operations can be performed on "dns-aaaaRec":

add| show| rm|

add dns aaaaRec

Creates a AAAA address record for the specified domain name. You cannot modify a AAAA address record.

Synopsis

add dns aaaaRec <hostName> <IPv6Address> ...

Arguments

hostName Domain name.

IPv6Address One or more IPv6 addresses to assign to the domain name.

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

Example

add dns aaaarec www.mynw.com 3::4:5 -ttl 10

show dns aaaaRec

Displays the AAAA (IPv6) address record for the specified host name. If a hostname is not specified, all configured AAAA records are shown.

Synopsis

show dns aaaaRec

Arguments

hostName Domain name.

IPv6Address One or more IPv6 addresses to assign to the domain name.

type Type of records to display. Available settings function as follows:

- ADNS - Display all authoritative address records.
- PROXY - Display all proxy address records.
- ALL - Display all address records.

Possible values: ALL, ADNS, PROXY

Output

ecsSubnet Subnet for which this particular record is cached. Subnet caching will occur for responses with EDNS Client Subnet (ECS) option. Applies to resource records obtained through proxy configurations only.

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600.

vServerName Vitual server name.

authType Authentication type.

devno count stateflag

rm dns aaaaRec

Removes an IPv6 address from a AAAA address record. The associated domain name must be specified. For EDNS Client Subnet (ECS) records, a subnet needs to be specified to remove an IPV6 address from a AAAA address record which is cached for that particular subnet. If no IPv6 address is specified, all AAAA records that belong to the specified domain name are removed.

Synopsis

rm dns aaaaRec <hostName> [-ecsSubnet <ip_addr|ipv6_addr>]

Arguments

hostName Domain name.

ecsSubnet Subnet for which the cached records need to be removed.

IPv6Address IPv6 address(es) of the AAAA record(s) to remove from the specified domain name.

Example

rm dns aaaarec www.mynw.com

dns-action

The following operations can be performed on "dns-action":

rm| unset| show| add| set|

rm dns action

Removes a dns Action.

Synopsis

rm dns action <actionName>

Arguments

actionName Name of the dns action.

Example

rm dns action action1

unset dns action

Use this command to remove dns action settings.Refer to the set dns action command for meanings of the arguments.

Synopsis

unset dns action <actionName>

show dns action

Used to display the action-related information.

Synopsis

show dns action

Arguments

actionName Name of the dns action.

Output

actionType The type of DNS action that is being configured.

TTL Time to live, in seconds.

IPAddress List of IP address to be returned in case of rewrite_response actiontype. They can be of IPV4 or IPV6 type. In case of set command We will remove all the IP address previously present in the action and will add new once given in set dns action command.

viewName The view name that must be used for the given action.

preferredLocList The location list in priority order used for the given action.

drop The dns packet must be dropped.

cacheBypass By pass dns cache for this.

dnsProfileName Name of the DNS profile to be associated with the transaction for which the action is chosen

builtin Flag to determine whether DNS action is default or not

feature The feature to be checked while applying this config

devno count stateflag

Example

show dns action <Action-Name> show dns action action1 show dns action

add dns action

Add a dns action.

Synopsis

add dns action <actionName> <actionType>

Arguments

actionName Name of the dns action.

actionType The type of DNS action that is being configured.

Possible values: ViewName, GslbPrefLoc, noop, Drop, Cache_Bypass, Rewrite_Response

IPAddress List of IP address to be returned in case of rewrite_response actiontype. They can be of IPV4 or IPV6 type. In case of set command We will remove all the IP address previously present in the action and will add new once given in set dns action command.

TTL Time to live, in seconds. Default value: 3600 Maximum value: 2147483647

viewName The view name that must be used for the given action.

preferredLocList The location list in priority order used for the given action.

dnsProfileName Name of the DNS profile to be associated with the transaction for which the action is chosen

Example

add dns action <actionName> <actionType> (-IPAddress <ip_addr|ipv6_addr> ... | -viewName <string> | -preferredLocList <string> ...) add dns action action1 Rewrite_Response -ipAddress 10.102.27.153 10.102.27.154 33::33 44::44 -TTL 4000 add dns action action1 GslbPrefLoc -preferredLocList india.10.102.81.175.80 us.10.102.81.176.80 add dns action action1 ViewName -viewName dnsview1

set dns action

Set a dns Action. Use this command to set the values for Ip address and TTL, If Ipaddress is given in set dns action command we will discard the previous set and will apply this new set of ipaddress given.

Synopsis

set dns action <actionName>

Arguments

actionName Name of the dns action.

IPAddress List of IP address to be returned in case of rewrite_response actiontype. They can be of IPV4 or IPV6 type. In case of set command We will remove all the IP address previously present in the action and will add new once given in set dns action command.

TTL Time to live, in seconds. Default value: 3600 Maximum value: 2147483647

viewName The view name that must be used for the given action.

preferredLocList The location list in priority order used for the given action.

dnsProfileName Name of the DNS profile to be associated with the transaction for which the action is chosen

Example

set dns action <actionName> set dns action action1 -ipAddress 10.102.27.153 10.102.27.154 33::33 44::44 -TTL 4000 set dns action action1 -viewName dnsview2 set dns action action1 -preferredLocList india.10.102.81.175.80

dns-action64

The following operations can be performed on "dns-action64":

set| add| rm| unset| show|

set dns action64

Set a DNS64 Action

Synopsis

set dns action64 <actionName>

Arguments

actionName Name of the dns64 action.

Prefix The dns64 prefix to be used if the after evaluating the rules

mappedRule The expression to select the criteria for ipv4 addresses to be used for synthesis. Only if the mappedrule is evaluated to true the corresponding ipv4 address is used for synthesis using respective prefix, otherwise the A RR is discarded

excludeRule The expression to select the criteria for eliminating the corresponding ipv6 addresses from the response.

Example

set dns dns64action -prefix -mappedrule -excluderule

add dns action64

Add a dns64 action.

Synopsis

add dns action64 <actionName> -Prefix <ipv6_addr|*>

Arguments

actionName Name of the dns64 action.

Prefix The dns64 prefix to be used if the after evaluating the rules

mappedRule The expression to select the criteria for ipv4 addresses to be used for synthesis. Only if the mappedrule is evaluated to true the corresponding ipv4 address is used for synthesis using respective prefix, otherwise the A RR is discarded

excludeRule The expression to select the criteria for eliminating the corresponding ipv6 addresses from the response.

Example

add dns dns64action <actionName> -prefix f23d:f43e::0/32

rm dns action64

Removes a dns64 Action.

Synopsis

rm dns action64 <actionName>

Arguments

actionName Name of the dns64 action.

Example

rm dns dns64action action1

unset dns action64

Use this command to remove dns action64 settings.Refer to the set dns action64 command for meanings of the arguments.

Synopsis

unset dns action64 <actionName>

show dns action64

Used to display the action-related information.

Synopsis

show dns action64

Arguments

actionName Name of the dns64 action.

Output

Prefix The dns64 prefix to be used if the after evaluating the rules

mappedRule The expression to select the criteria for ipv4 addresses to be used for synthesis. Only if the mappedrule is evaluated to true the corresponding ipv4 address is used for synthesis using respective prefix, otherwise the A RR is discarded

excludeRule The expression to select the criteria for eliminating the corresponding ipv6 addresses from the response.

builtin Flag to determine whether dna64action is default or not

feature The feature to be checked while applying this config

devno count stateflag

Example

show dns dns64action

dns-addRec

The following operations can be performed on "dns-addRec":

add| rm| show|

add dns addRec

Creates an IPv4 address record for the specified domain name. You cannot modify an address resource record.

Synopsis

add dns addRec <hostName> <IPAddress> ...

Arguments

hostName Domain name.

IPAddress One or more IPv4 addresses to assign to the domain name.

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

Example

Add dns addrec www.mynw.com 65.200.211.139 -ttl 10

rm dns addRec

Removes an IPv4 address from an address record. The associated domain name must be specified. For EDNS Client Subnet (ECS) records, a subnet needs to be specified to remove an IPV4 address from an address record which is cached for that particular subnet. If no IPv4 address is specified, all records that belong to the specified domain name are removed.

Synopsis

rm dns addRec <hostName> [-ecsSubnet <ip_addr|ipv6_addr>]

Arguments

hostName Domain name.

ecsSubnet Subnet for which the cached address records need to be removed.

IPAddress IPv4 address(es) of the address records to remove from the specified domain name.

Example

rm dns addrec www.mynw.com

show dns addRec

Displays the IPv4 address record for the specified host name. If a hostname is not specified, all configured address records are shown.

Synopsis

show dns addRec

Arguments

hostName Domain name.

type The address record type. The type can take 3 values: ADNS - If this is specified, all of the authoritative address records will be displayed. PROXY - If this is specified, all of the proxy address records will be displayed. ALL - If this is specified, all of the address records will be displayed.

Possible values: ALL, ADNS, PROXY

Output

IPAddress IP addresses for the domain name.

ecsSubnet Subnet for which this particular record is cached. Subnet caching will occur for responses with EDNS Client Subnet (ECS) option. Applies to resource records obtained through proxy configurations only.

TTL The time to live, in seconds.

vServerName Vitual server name.

authType Authentication type.

devno count stateflag

dns-caaRec

The following operations can be performed on "dns-caaRec":

add| rm| show|

add dns caaRec

Creates a CAA record for the specified domain name. Each resource record is stored with a unique, internally generated record ID, which you can view and use to delete the record. You cannot modify a CAA resource record.

Synopsis

add dns caaRec <domain> <valueString>

Arguments

domain Domain name of the CAA record.

valueString Value associated with the chosen property tag in the CAA resource record. Enclose the string in single or double quotation marks.

tag String that represents the identifier of the property represented by the CAA record. The RFC currently defines three available tags - issue, issuwild and iodef. Default value: "issue"

flag Flag associated with the CAA record.

Possible values: NONE, CRITICAL Default value: 5

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

Example

add dns caaRec certs.example.com ca1.example.net -tag issue add dns caaRec wild.example.com ca2.example.net -tag issuwild

rm dns caaRec

Removes the specified CAA record from the specified domain. For EDNS Client Subnet (ECS) records, a subnet needs to be specified to remove a CAA record which is cached for that particular subnet.

Synopsis

rm dns caaRec <domain> ((<valueString>) | -recordId <positive_integer>@) [-ecsSubnet <ip_addr |ipv6_addr>]

Arguments

domain Domain name of the CAA record.

valueString Value associated with the chosen property tag in the CAA resource record. Enclose the string in single or double quotation marks.

recordId Unique, internally generated record ID. View the details of the CAA record to obtain its record ID. Records can be removedby either specifying the domain name and record id OR by specifying domain name and all other CAA record attributes as was supplied during the add command. Minimum value: 1 Maximum value: 65535

tag String that represents the identifier of the property represented by the CAA record. The RFC currently defines three available tags - issue, issuwild and iodef. Default value: "issue"

flag Flag associated with the CAA record.

Possible values: NONE, CRITICAL Default value: 5

ecsSubnet Subnet for which the cached CAA record need to be removed.

Example

rm dns caaRec certs.example.com ca1.example.net -tag issue rm dns caaRec wild.example.com ca2.example.net -tag issuwild

show dns caaRec

Displays CAA records owned by the specified domain. If no domain name is specified, all configured CAA records are shown.

Synopsis

show dns caaRec

Arguments

domain Domain name of the CAA record.

type Type of records to display. Available settings function as follows:

- ADNS - Display all authoritative address records.
- PROXY - Display all proxy address records.
- ALL - Display all address records.

Possible values: ALL, ADNS, PROXY Default value: ADNS

Output

valueString Value associated with the chosen property tag in the CAA resource record. Enclose the string in single or double quotation marks.

tag String that represents the identifier of the property represented by the CAA record. The RFC currently defines three available tags - issue, issuwild and iodef.

flag Flag associated with the CAA record.

ecsSubnet Subnet for which this particular record is cached. Subnet caching will occur for responses with EDNS Client Subnet (ECS) option. Applies to resource records obtained through proxy configurations only

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600.

recordId authType Authentication type.

devno count stateflag

Example

show dns caaRec certs.example.com show dns caaRec

dns-cnameRec

The following operations can be performed on "dns-cnameRec":

add| show| rm|

add dns cnameRec

Creates a canonical name (CNAME) record, or alias, for the specified domain name.

Synopsis

add dns cnameRec <aliasName> <canonicalName>

Arguments

aliasName Alias for the canonical domain name.

canonicalName Canonical domain name.

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

Example

add dns cnameRec www.mynw.org www.mynw.com -ttl 20

show dns cnameRec

Displays the canonical name (CNAME) records configured for the specified alias. If no alias is specified, all configured CNAME records are displayed

Synopsis

show dns cnameRec

Arguments

aliasName Alias for which to display CNAME records.

type Type of records to display. Available settings function as follows:

- ADNS - Display all authoritative address records.
- PROXY - Display all proxy address records.
- ALL - Display all address records.

Possible values: ALL, ADNS, PROXY Default value: ADNS

Output

canonicalName Canonical domain name.

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600.

vServerName GSLB Vitual server name to which this domain is bound

authType Record type.

ecsSubnet Subnet for which this particular record is cached. Subnet caching will occur for responses with EDNS Client Subnet (ECS) option. Applies to resource records obtained through proxy configurations only.

devno count stateflag

Example

show dns cnameRec www.mynw.org

rm dns cnameRec

Removes a canonical name (CNAME) record. For EDNS Client Subnet (ECS) records, a subnet needs to be specified to remove a CNAME record which is cached for that particular subnet

Synopsis

rm dns cnameRec <aliasName> [-ecsSubnet <ip_addr|ipv6_addr>]

Arguments

aliasName Alias for which to remove the CNAME record.

ecsSubnet Subnet for which the cached CNAME record need to be removed.

Example

rm dns cnamerec www.mynw.org

Dns

The entities on which you can perform NetScaler CLI operations:

- dns-aaaaRec
- dns-action
- dns-action64
- dns-addRec
- dns-caaRec
- dns-cnameRec
- dns
- dns-global
- dns-key
- dns-mxRec
- dns-nameServer
- dns-naptrRec
- dns-nsRec
- dns-nsecRec
- dns-parameter
- dns-policy
- dns-policy64
- dns-policylabel
- dns-profile
- dns-proxyRecords
- dns-ptrRec
- dns-records
- dns-soaRec
- dns-srvRec
- dns-stats
- dns-subnetcache
- dns-suffix

- dns-txtRec
- dns-view
- dns-zone

dns-global

The following operations can be performed on "dns-global":

bind| show| unbind|

bind dns global

Binds the specified DNS policy globally.

Synopsis

bind dns global <policyName> <priority>

Arguments

policyName Name of the DNS policy to bind globally.

priority Integer specifying the policy's priority. The lower the number, the higher the priority. Minimum value: 1

gotoPriorityExpression Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.

- If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

type Type of global bind point to which to bind the DNS policy.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

invoke Invoke flag.

labelType Type of policy label invocation.

Possible values: policylabel

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

Example

bind dns global pol9 9

show dns global

Displays the DNS policies bound to the specified global bind point. If a global bind point is not specified, the command displays the global bind points that have policies bound to them, and the number of policies bound to each of those bind points.

Synopsis

show dns global

Arguments

type Type of global bind point for which to show bound policies.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

Output

stateflag policyName Name of the dns policy.

priority Specifies the priority of the policy with which it is bound. Maximum allowed priority should be less than 65535

gotoPriorityExpression Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

invoke Invoke flag.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

numpol The number of policies bound to the bindpoint.

flowType flowtype of the bound rewrite policy.

flags upgraded It is internally used to tell that the policy is a upgraded policy.

builtin Flag to determine whether DNS policy binding is default or not

feature The feature to be checked while applying this config

globalBindType devno count

Example

show dns global show dns global -type REQ_DEFAULT show dns global -type RES_DEFAULT

unbind dns global

Unbinds the specified DNS policy from the global bind point.

Synopsis

unbind dns global <policyName>

Arguments

policyName Name of the DNS policy to unbind.

type Type of global bind point to which to bind the DNS policy.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

Example

unbind dns global pol9

dns-key

The following operations can be performed on "dns-key":

set| rm| add| show| create| unset| import|

set dns key

Modifies the specified parameters of a DNS key. Note: If you change the expiry time period of a key, the Citrix ADC, using the modified key, automatically re-signs all the resource records in the zone, provided that the zone is currently signed with the particular key.

Synopsis

set dns key <keyName> [-expires <positive_integer>] [-notificationPeriod <positive_integer>]

Arguments

keyName Name of the public-private key pair.

expires Time period for which to consider the key valid, after the key is used to sign a zone. Default value: 120 Minimum value: 1 Maximum value: 32767

units Units for the expiry period.

Possible values: MINUTES, HOURS, DAYS Default value: DAYS

notificationPeriod Time at which to generate notification of key expiration, specified as number of days, hours, or minutes before expiry. Must be less than the expiry period. The notification is an SNMP trap sent to an SNMP manager. To enable the appliance to send the trap, enable the DNSKEY-EXPIRY SNMP alarm. Default value: 7 Minimum value: 1 Maximum value: 32767

units Units for the notification period.

Possible values: MINUTES, HOURS, DAYS Default value: DAYS

TTL Time to Live (TTL), in seconds, for the DNSKEY resource record created in the zone. TTL is the time for which the record must be cached by the DNS proxies. If the TTL is not specified, either the DNS zone's minimum TTL or the default value of 3600 is used. Default value: 3600 Maximum value: 2147483647

Example

add dns key secure.example.zsk -public secure.example-rsasha1-1024.key -private /nsconfig/dns/secure.example-rsasha1-1024.private

rm dns key

Removes a DNS key.

Synopsis

rm dns key <keyName>

Arguments

keyName Name of the public-private key pair.

Example

rm dns key secure.example.zsk

add dns key

Adds a DNS key to the zone that is specified in the key file.

Synopsis

add dns key <keyName> <publickey> <privatekey> [-expires <positive_integer>] [-notificationPeriod <positive_integer>] {-password }

Arguments

keyName Name of the public-private key pair to publish in the zone.

publickey File name of the public key.

privatekey File name of the private key.

expires Time period for which to consider the key valid, after the key is used to sign a zone. Default value: 120 Minimum value: 1 Maximum value: 32767

units Units for the expiry period.

Possible values: MINUTES, HOURS, DAYS Default value: DAYS

notificationPeriod Time at which to generate notification of key expiration, specified as number of days, hours, or minutes before expiry. Must be less than the expiry period. The notification is an SNMP trap sent to an SNMP manager. To enable the appliance to send the trap, enable the DNSKEY-EXPIRY SNMP alarm. Default value: 7 Minimum value: 1 Maximum value: 32767

units Units for the notification period.

Possible values: MINUTES, HOURS, DAYS Default value: DAYS

TTL Time to Live (TTL), in seconds, for the DNSKEY resource record created in the zone. TTL is the time for which the record must be cached by the DNS proxies. If the TTL is not specified, either the DNS zone's minimum TTL or the default value of 3600 is used. Default value: 3600 Maximum value: 2147483647

password Passphrase for reading the encrypted public/private DNS keys

Example

add dns key secure.example.zsk -public secure.example-rsasha1-1024.key -private /nsconfig/dns/secure.example-rsasha1-1024.private

show dns key

Displays the parameters of the specified DNS key. If no DNS key name is specified, all configured DNS keys are shown. Note: You cannot view the parameters of a public/private key file. You can view the parameters of a key after you have published it in a DNS zone by using either the add dns key command or the DNS > Zones > Sign/Unsign DNS Zone dialog box.

Synopsis

show dns key

Arguments

keyName Name of the public-private key pair.

Output

publickey File name of the public key.

privatekey File name of the private key.

expires Number of days since signing with this key, when the key expires.

units Units for the expiry period.

notificationPeriod Time at which to generate notification of key expiration, specified as number of days, hours, or minutes before expiry. Must be less than the expiry period. The notification is an SNMP trap sent to an SNMP manager. To enable the appliance to send the trap, enable the DNSKEY-EXPIRY SNMP alarm.

units Units for the notification period.

TTL Time to Live (TTL), in seconds, for the DNSKEY resource record created in the zone. TTL is the time for which the record must be cached by the DNS proxies. If the TTL is not specified, either the DNS zone's minimum TTL or the default value of 3600 is used.

zoneName Name of the zone for which the key is created.

password Passphrase for reading the encrypted public/private DNS keys

devno count stateflag

Example

show dns key

create dns key

Creates a public-private key pair to use for signing a DNS zone. The keys are created in the /nsconfig/dns/ directory on the Citrix ADC. The private, pubic, and DS key files are created with names having the format ..

Synopsis

create dns key -zoneName <string> -keyType <keyType> -algorithm <algorithm> -keySize <positive_integer> -fileNamePrefix <string> {-password }

Arguments

zoneName Name of the zone for which to create a key.

keyType Type of key to create.

Possible values: KSK, KeySigningKey, ZSK, ZoneSigningKey Default value: NS_DNSKEY_ZSK

algorithm Algorithm to generate for zone signing.

Possible values: RSASHA1, RSASHA256, RSASHA512 Default value: NS_DNSKEYALGO_RSASHA1

keySize Size of the key, in bits. Default value: 512 Minimum value: 1 Maximum value: 4096

fileNamePrefix Common prefix for the names of the generated public and private key files and the Delegation Signer (DS) resource record. During key generation, the .key, .private, and .ds suffixes are appended automatically to the file name prefix to produce the names of the public key, the private key, and the DS record, respectively.

password Passphrase for reading the encrypted public/private DNS keys

Example

create dns key -zone dnssec.bar -algorithm RSASHA1 -keySize 1024

unset dns key

Use this command to remove dns key settings.Refer to the set dns key command for meanings of the arguments.

Synopsis

unset dns key <keyName>

import dns key

Import the DNSSEC key.

Synopsis

import dns key <keyName> -src <URL>

Arguments

keyName Name of the public-private key pair to publish in the zone.

src URL (protocol, host, path, and file name) from where the DNS key file will be imported. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access. This is a mandatory argument

dns-mxRec

The following operations can be performed on "dns-mxRec":

add| set| show| rm| unset|

add dns mxRec

Creates a mail exchange (MX) record for the specified domain name.

Synopsis

add dns mxRec <domain> -mx <string> -pref <positive_integer>

Arguments

domain Domain name for which to add the MX record.

mx Host name of the mail exchange server.

pref Priority number to assign to the mail exchange server. A domain name can have multiple mail servers, with a priority number assigned to each server. The lower the priority number, the higher the mail server's priority. When other mail servers have to deliver mail to the specified domain, they begin with the mail server with the lowest priority number, and use other configured mail servers, in priority order, as backups. Minimum value: 0 Maximum value: 65535

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

set dns mxRec

Modifies the priority number and TTL of the mail exchange (MX) record.

Synopsis

set dns mxRec <domain> -mx <string>

Arguments

domain Domain of the MX record to be modified.

mx Host name of the mail exchange server to be modified.

pref Priority number to assign to the mail exchange server. A domain name can have multiple mail servers, with a priority number assigned to each server. The lower the priority number, the higher the mail server's priority. When other mail servers have to deliver mail to the specified domain, they begin with the mail server with the lowest priority number, and use other configured mail servers, in priority order, as backups. Minimum value: 0 Maximum value: 65535

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

show dns mxRec

Displays the mail exchange (MX) records for the specified domain. If no domain name is specified, all configured mail exchange records are shown.

Synopsis

show dns mxRec

Arguments

domain Domain name.

type Type of records to display. Available settings function as follows:

- ADNS - Display all authoritative address records.
- PROXY - Display all proxy address records.
- ALL - Display all address records.

Possible values: ALL, ADNS, PROXY Default value: ADNS

Output

mx Host name of the mail exchange server.

pref Priority number to assign to the mail exchange server. A domain name can have multiple mail servers, with a priority number assigned to each server. The lower the priority number, the higher the mail server's priority. When other mail servers have to deliver mail to the specified domain, they begin with the mail server with the lowest priority number, and use other configured mail servers, in priority order, as backups.

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600.

authType Record type.

ecsSubnet Subnet for which this particular record is cached. Subnet caching will occur for responses with EDNS Client Subnet (ECS) option. Applies to resource records obtained through proxy configurations only.

devno count stateflag

rm dns mxRec

Removes the specified mail exchange (MX) record from the specified domain. For EDNS Client Subnet (ECS) records, a subnet needs to be specified to remove the specified mail exchange (MX) record which is cached for that particular subnet

Synopsis

rm dns mxRec <domain> <mx> [-ecsSubnet <ip_addr|ipv6_addr>]

Arguments

domain Domain name.

mx Host name of the mail exchange server.

ecsSubnet Subnet for which the cached MX record need to be removed.

unset dns mxRec

Use this command to remove dns mxRec settings.Refer to the set dns mxRec command for meanings of the arguments.

Synopsis

unset dns mxRec <domain> -mx <string> -TTL

dns-nameServer

The following operations can be performed on "dns-nameServer":

enable| rm| disable| add| show| unset| set|

enable dns nameServer

Enables a name server.

Synopsis

enable dns nameServer (<IP> | <dnsVserverName> | -type <type>)

Arguments

IP IP address of the name server.

dnsVserverName Name of the DNS virtual server.

type Protocol used by the name server. UDP_TCP is not valid if the name server is a DNS virtual server configured on the appliance.

Possible values: UDP, TCP, UDP_TCP Default value: UDP

Example

enable dns nameserver 10.14.43.149

rm dns nameServer

Removes a name server from the Citrix ADC. If the name server is an IP-address based external name server, the name server entry is removed. If the name server is a DNS virtual server on the appliance, the virtual server is not removed, but it is no longer used to resolve domain names.

Synopsis

rm dns nameServer (<IP> | <dnsVserverName> | -type <type>)

Arguments

IP IP address of the name server.

dnsVserverName Name of the DNS virtual server.

type Protocol used by the name server. UDP_TCP is not valid if the name server is a DNS virtual server configured on the appliance.

Possible values: UDP, TCP, UDP_TCP Default value: UDP

Example

Deleting an IP-based nameserver: rm nameserver 10.102.4.1, Deleting a vserver-based nameserver: rm nameserver dns_vsvr

disable dns nameServer

Disables a name server.

Synopsis

disable dns nameServer (<IP> | <dnsVserverName> | -type <type>)

Arguments

IP IP address of the name server.

dnsVserverName Name of the DNS virtual server.

type Protocol used by the name server. UDP_TCP is not valid if the name server is a DNS virtual server configured on the appliance.

Possible values: UDP, TCP, UDP_TCP Default value: UDP

Example

disable dns nameserver 10.14.43.149

add dns nameServer

Adds a name server to the appliance. Following are the two types of name servers that can be added:

- IP address-based name server - An external name server to contact for domain name resolution. If multiple IP address-based name servers are configured on the appliance, and the local parameter is not set on any of them, incoming DNS queries are load balanced across all the name servers, in round robin fashion.
- Virtual server-based name server - A DNS virtual server configured in the Citrix ADC. If you want more fine-grained control on how external DNS name servers are load balanced (for example, you want a load balancing method other than round robin), you configure a DNS virtual server on the appliance, bind the external name servers as its services, and then specify the name of the virtual server in this command.

Synopsis

add dns nameServer ((<IP>) | <dnsVserverName>)

Arguments

IP IP address of an external name server or, if the Local parameter is set, IP address of a local DNS server (LDNS).

dnsVserverName Name of a DNS virtual server. Overrides any IP address-based name servers configured on the Citrix ADC.

local Mark the IP address as one that belongs to a local recursive DNS server on the Citrix ADC. The appliance recursively resolves queries received on an IP address that is marked as being local. For recursive resolution to work, the global DNS parameter, Recursion, must also be set.

If no name server is marked as being local, the appliance functions as a stub resolver and load balances the name servers.

state Administrative state of the name server.

Possible values: ENABLED, DISABLED Default value: ENABLED

type Protocol used by the name server. UDP_TCP is not valid if the name server is a DNS virtual server configured on the appliance.

Possible values: UDP, TCP, UDP_TCP Default value: UDP

dnsProfileName Name of the DNS profile to be associated with the name server

Example

Adding an-IP based nameserver IP: add nameserver 10.102.4.1, Adding a vserver-based name server: add nameserver dns_vsvr where dns_vsvr is the name of a DNS vserver created in the system.

show dns nameServer

Displays the name servers configured on the Citrix ADC, along with their administrative states.

Synopsis

show dns nameServer

Arguments

IP IP address of the name server.

dnsVserverName Name of the DNS virtual server.

Output

serviceName The name of the dns vserver.

port Port of the service.

type Protocol used by the name server. UDP_TCP is not valid if the name server is a DNS virtual server configured on the appliance.

state Administrative state of the name server.

nameserverstate State of the server.

local ip is a local recursive nameserver.

adminState ClMonOwner Tells the mon owner of the service.

ClMonView Tells the view id by which state of the service is updated.

dnsProfileName Name of the DNS profile to be associated with the name server

devno count stateflag

unset dns nameServer

Use this command to remove dns nameServer settings.Refer to the set dns nameServer command for meanings of the arguments.

Synopsis

unset dns nameServer <IP>

set dns nameServer

Modifies the attributes of a DNS name server. Only IP based name server entities can be modified using this command. If the DNS name server is an LB VServer, modification to any of the attributes should be done using set lb vserver command

Synopsis

set dns nameServer <IP>

Arguments

IP IP address of an external name server or, if the Local parameter is set, IP address of a local DNS server (LDNS).

dnsProfileName Name of the DNS profile to be associated with the name server

type Protocol used by the name server. UDP_TCP is not valid if the name server is a DNS virtual server configured on the appliance.

Possible values: UDP, TCP, UDP_TCP Default value: UDP

Example

set dns nameserver 1.1.1.1 -dnsprofilename test2

dns-naptrRec

The following operations can be performed on "dns-naptrRec":

show| rm| add|

show dns naptrRec

Displays NAPTR records owned by the specified domain. If no domain name is specified, all configured NAPTR records are shown.

Synopsis

show dns naptrRec

Arguments

domain Name of the domain for the NAPTR record.

type Type of records to display. Available settings function as follows:

- ADNS - Display all authoritative address records.
- PROXY - Display all proxy address records.
- ALL - Display all address records.

Possible values: ALL, ADNS, PROXY Default value: ADNS

Output

order An integer specifying the order in which the NAPTR records MUST be processed in order to accurately represent the ordered list of Rules. The ordering is from lowest to highest

preference An integer specifying the preference of this NAPTR among NAPTR records having same order. lower the number, higher the preference.

flags flags for this NAPTR.

services Service Parameters applicable to this delegation path.

regexp The regular expression, that specifies the substitution expression for this NAPTR

replacement The replacement domain name for this NAPTR.

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the

same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600.

recordId authType Authentication type.

ecsSubnet Subnet for which this particular record is cached. Subnet caching will occur for responses with EDNS Client Subnet (ECS) option. Applies to resource records obtained through proxy configurations only.

vServerName Virtual server name.

devno count stateflag

Example

show dns naptrRec spf.m.test. show dns naptrRec

rm dns naptrRec

Removes the specified NAPTR record from the specified domain. For EDNS Client Subnet (ECS) records, a subnet needs to be specified to remove a NAPTR record which is cached for that particular subnet

Synopsis

rm dns naptrRec <domain> ((<order> <preference> (-regexp <expression> | -replacement <string>)) | -recordId <positive_integer>@) [-ecsSubnet <ip_addr|ipv6_addr>]

Arguments

domain Name of the domain for the NAPTR record.

order An integer specifying the order in which the NAPTR records MUST be processed in order to accurately represent the ordered list of Rules. The ordering is from lowest to highest Minimum value: 0 Maximum value: 65535

recordId Unique, internally generated record ID. View the details of the naptr record to obtain its record ID. Records can be removed by either specifying the domain name and record id OR by specifying domain name and all other naptr record attributes as was supplied during the add command. Minimum value: 1 Maximum value: 65535

ecsSubnet Subnet for which the cached NAPTR record need to be removed.

preference An integer specifying the preference of this NAPTR among NAPTR records having same order. lower the number, higher the preference. Minimum value: 0 Maximum value: 65535

flags flags for this NAPTR.

services Service Parameters applicable to this delegation path.

regexp The regular expression, that specifies the substitution expression for this NAPTR

replacement The replacement domain name for this NAPTR.

Example

TBD

add dns naptrRec

Creates an NAPTR record. Each resource record is stored with a unique, internally generated record ID, which you can view and use to delete the record.

Synopsis

add dns naptrRec <domain> <order> <preference> (-regexp <expression> | -replacement <string>)

Arguments

domain Name of the domain for the NAPTR record.

order An integer specifying the order in which the NAPTR records MUST be processed in order to accurately represent the ordered list of Rules. The ordering is from lowest to highest Minimum value: 0 Maximum value: 65535

preference An integer specifying the preference of this NAPTR among NAPTR records having same order. lower the number, higher the preference. Minimum value: 0 Maximum value: 65535

flags flags for this NAPTR.

services Service Parameters applicable to this delegation path.

regexp The regular expression, that specifies the substitution expression for this NAPTR

replacement The replacement domain name for this NAPTR.

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

Example

TBD

dns-nsRec

The following operations can be performed on "dns-nsRec":

show| rm| add|

show dns nsRec

Displays the name server records for the specified domain. If no domain name is specified, all configured name server records are shown.

Synopsis

show dns nsRec

Arguments

domain Domain name.

type Type of records to display. Available settings function as follows:

- ADNS - Display all authoritative address records.
- PROXY - Display all proxy address records.
- ALL - Display all address records.

Possible values: ALL, ADNS, PROXY

Output

nameServer Host name of the name server to add to the domain.

ecsSubnet Subnet for which this particular record is cached. Subnet caching will occur for responses with EDNS Client Subnet (ECS) option. Applies to resource records obtained through proxy configurations only.

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600.

authType Record type.

devno count stateflag

rm dns nsRec

Removes the specified name server record from the specified domain. For EDNS Client Subnet (ECS) records, a subnet needs to be specified to remove the specified name server record from the specified domain which is cached for that particular subnet

Synopsis

rm dns nsRec <domain> <nameServer> [-ecsSubnet <ip_addr|ipv6_addr>]

Arguments

domain Domain name.

nameServer Name server to remove.

ecsSubnet Subnet for which the cached name server record need to be removed.

add dns nsRec

Creates a name server record for the specified domain.

Synopsis

add dns nsRec <domain> <nameServer>

Arguments

domain Domain name.

nameServer Host name of the name server to add to the domain.

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

dns-nsecRec

The following operations can be performed on "dns-nsecRec":

show dns nsecRec

Displays the NextSECure (NSEC) resource records created for the specified domain name.

Synopsis

show dns nsecRec

Arguments

hostName Name of the domain.

type Type of records to display. Available settings function as follows:

- ADNS - Display all authoritative address records.
- PROXY - Display all proxy address records.
- ALL - Display all address records.

Possible values: ALL, ADNS, PROXY

Output

nextNsec Next nsec record in the chain

nsecBitarray Bit array representing the different record types configured for the domain name

nextRecs An array of record types associated with the nsec record.

TTL Time to Live (TTL), in seconds, for the record.

ecsSubnet Subnet for which this particular record is cached. Subnet caching will occur for responses with EDNS Client Subnet (ECS) option. Applies to resource records obtained through proxy configurations only.

devno count stateflag

Example

show dns nsecRec foo.bar

dns-parameter

The following operations can be performed on "dns-parameter":

show| unset| set|

show dns parameter

Displays the global DNS parameters.

Synopsis

show dns parameter

Arguments

Output

retries Maximum number of retry attempts when no response is received for a query sent to a name server. Applies to end resolver and forwarder configurations.

minTTL Minimum permissible time to live (TTL) for all records cached in the DNS cache by DNS proxy, end resolver, and forwarder configurations. If the TTL of a record that is to be cached is lower than the value configured for minTTL, the TTL of the record is set to the value of minTTL before caching. When you modify this setting, the new value is applied only to those records that are cached after the modification. The TTL values of existing records are not changed.

maxTTL Maximum time to live (TTL) for all records cached in the DNS cache by DNS proxy, end resolver, and forwarder configurations. If the TTL of a record that is to be cached is higher than the value configured for maxTTL, the TTL of the record is set to the value of maxTTL before caching. When you modify this setting, the new value is applied only to those records that are cached after the modification. The TTL values of existing records are not changed.

nameLookupPriority Type of lookup (DNS or WINS) to attempt first. If the first-priority lookup fails, the second-priority lookup is attempted. Used only by the SSL VPN feature.

cacheRecords Cache resource records in the DNS cache. Applies to resource records obtained through proxy configurations only. End resolver and forwarder configurations always cache records in the DNS cache, and you cannot disable this behavior. When you disable record caching, the appliance stops caching server responses. However, cached records are not flushed. The appliance does not serve requests from the cache until record caching is enabled again.

recursion Function as an end resolver and recursively resolve queries for domains that are not hosted on the Citrix ADC. Also resolve queries recursively when the external name servers configured on the appliance (for a forwarder configuration) are unavailable. When external name servers are unavailable, the appliance queries a root server and resolves the request recursively, as it does for an end resolver configuration.

resolutionOrder Type of DNS queries (A, AAAA, or both) to generate during the routine functioning of certain Citrix ADC features, such as SSL VPN, cache redirection, and the integrated cache. The queries are sent to the external name servers that are configured for the forwarder function. If you specify both query types, you can also specify the order. Available settings function as follows:

- OnlyAQuery. Send queries for IPv4 address records (A records) only.
- OnlyAAAAQuery. Send queries for IPv6 address records (AAAA records) instead of queries for IPv4 address records (A records).
- AThenAAAAQuery. Send a query for an A record, and then send a query for an AAAA record if the query for the A record results in a NODATA response from the name server.
- AAAAThenAQuery. Send a query for an AAAA record, and then send a query for an A record if the query for the AAAA record results in a NODATA response from the name server.

dnssec Enable or disable the Domain Name System Security Extensions (DNSSEC) feature on the appliance. Note: Even when the DNSSEC feature is enabled, forwarder configurations (used by internal Citrix ADC features such as SSL VPN and Cache Redirection for name resolution) do not support the DNSSEC OK (DO) bit in the EDNS0 OPT header.

maxPipeline Maximum value of the concurrent DNS pipeline. A setting of zero makes the pipeline infinite

dnsRootReferral Send a root referral if a client queries a domain name that is unrelated to the domains configured/cached on the Citrix ADC. If the setting is disabled, the appliance sends a blank response instead of a root referral. Applicable to domains for which the appliance is

authoritative. Disable the parameter when the appliance is under attack from a client that is sending a flood of queries for unrelated domains.

dns64Timeout While doing DNS64 resolution, this parameter specifies the time to wait before sending an A query if no response is received from backend DNS server for AAAA query.

ecsMaxSubnets Maximum number of subnets that can be cached corresponding to a single domain. Subnet caching will occur for responses with EDNS Client Subnet (ECS) option. Caching of such responses can be disabled using DNS profile settings. A value of zero indicates that the number of subnets cached is limited only by existing memory constraints. The default value is zero.

maxnegcacheTTL Maximum time to live (TTL) for all negative records (NXDONAIN and NODATA) cached in the DNS cache by DNS proxy, end resolver, and forwarder configurations. If the TTL of a record that is to be cached is higher than the value configured for maxnegcacheTTL, the TTL of the record is set to the value of maxnegcacheTTL before caching. When you modify this setting, the new value is applied only to those records that are cached after the modification. The TTL values of existing records are not changed.

cacheHitBypass This parameter is applicable only in proxy mode and if this parameter is enabled we will forward all the client requests to the backend DNS server and the response served will be cached on Citrix ADC

maxCacheSize Maximum memory, in megabytes, that can be used for dns caching per Packet Engine.

maxNegativeCacheSize Maximum memory, in megabytes, that can be used for caching of negative DNS responses per packet engine.

cacheNoExpire If this flag is set to YES, the existing entries in cache do not age out. On reaching the max limit the cache records are frozen

splitPktQueryProcessing Processing requests split across multiple packets

cacheECSZeroPrefix Cache ECS responses with a Scope Prefix length of zero. Such a cached response will be used for all queries with this domain name and any subnet. When disabled, ECS responses with Scope Prefix length of zero will be cached, but not tied to any subnet. This option has no effect if caching of ECS responses is disabled in the corresponding DNS profile.

maxUDPPacketSize Maximum UDP packet size that can be handled by Citrix ADC. This is the value advertised by Citrix ADC when responding as an authoritative server and it is also used when Citrix ADC queries other name servers as a forwarder. When acting as a proxy, requests

from clients are limited by this parameter - if a request contains a size greater than this value in the OPT record, it will be replaced.

builtin Flag to determine if dns param is built-in or not

feature The feature to be checked while applying this config

NXDomainRateLimitThreshold Rate limit threshold for Non-Existant domain (NXDOMAIN) responses generated from Citrix ADC. Once the threshold is breached , DNS queries leading to NXDOMAIN response will be dropped. This threshold will not be applied for NXDOMAIN responses got from the backend. The threshold will be applied per packet engine and per second.

NXDomainThresholdCrossed Number of times requests has been dropped as number of DNS queries leading to NXDOMAIN response has crossed the threshold

unset dns parameter

Use this command to remove dns parameter settings.Refer to the set dns parameter command for meanings of the arguments.

Synopsis

unset dns parameter

set dns parameter

Modifies global DNS parameters on the Citrix ADC.

Synopsis

set dns parameter

Arguments

retries Maximum number of retry attempts when no response is received for a query sent to a name server. Applies to end resolver and forwarder configurations. Default value: 5 Minimum value: 1 Maximum value: 5

minTTL Minimum permissible time to live (TTL) for all records cached in the DNS cache by DNS proxy, end resolver, and forwarder configurations. If the TTL of a record that is to be cached is lower than the value configured for minTTL, the TTL of the record is set to the value of minTTL before caching. When you modify this setting, the new value is applied only to those records that

are cached after the modification. The TTL values of existing records are not changed. Maximum value: 604800

maxTTL Maximum time to live (TTL) for all records cached in the DNS cache by DNS proxy, end resolver, and forwarder configurations. If the TTL of a record that is to be cached is higher than the value configured for maxTTL, the TTL of the record is set to the value of maxTTL before caching. When you modify this setting, the new value is applied only to those records that are cached after the modification. The TTL values of existing records are not changed. Default value: 604800 Minimum value: 1 Maximum value: 604800

nameLookupPriority Type of lookup (DNS or WINS) to attempt first. If the first-priority lookup fails, the second-priority lookup is attempted. Used only by the SSL VPN feature.

Possible values: WINS, DNS Default value: WINS

recursion Function as an end resolver and recursively resolve queries for domains that are not hosted on the Citrix ADC. Also resolve queries recursively when the external name servers configured on the appliance (for a forwarder configuration) are unavailable. When external name servers are unavailable, the appliance queries a root server and resolves the request recursively, as it does for an end resolver configuration.

Possible values: ENABLED, DISABLED Default value: DISABLED

resolutionOrder Type of DNS queries (A, AAAA, or both) to generate during the routine functioning of certain Citrix ADC features, such as SSL VPN, cache redirection, and the integrated cache. The queries are sent to the external name servers that are configured for the forwarder function. If you specify both query types, you can also specify the order. Available settings function as follows:

- OnlyAQuery. Send queries for IPv4 address records (A records) only.
- OnlyAAAAQuery. Send queries for IPv6 address records (AAAA records) instead of queries for IPv4 address records (A records).
- AThenAAAAQuery. Send a query for an A record, and then send a query for an AAAA record if the query for the A record results in a NODATA response from the name server.
- AAAAThenAQuery. Send a query for an AAAA record, and then send a query for an A record if the query for the AAAA record results in a NODATA response from the name server.

Possible values: OnlyAQuery, OnlyAAAAQuery, AThenAAAAQuery, AAAAThenAQuery Default value: OnlyAQuery

dnssec Enable or disable the Domain Name System Security Extensions (DNSSEC) feature on the appliance. Note: Even when the DNSSEC feature is enabled, forwarder configurations (used by internal Citrix ADC features such as SSL VPN and Cache Redirection for name resolution) do not support the DNSSEC OK (DO) bit in the EDNS0 OPT header.

Possible values: ENABLED, DISABLED Default value: ENABLED

maxPipeline Maximum number of concurrent DNS requests to allow on a single client connection, which is identified by the clientip:port-<vserver ip:port> tuple. A value of 0 (zero) applies no limit to the number of concurrent DNS requests allowed on a single client connection. Default value: NSNATPCB_MAXPIPELINE Minimum value: 0

dnsRootReferral Send a root referral if a client queries a domain name that is unrelated to the domains configured/cached on the Citrix ADC. If the setting is disabled, the appliance sends a blank response instead of a root referral. Applicable to domains for which the appliance is authoritative. Disable the parameter when the appliance is under attack from a client that is sending a flood of queries for unrelated domains.

Possible values: ENABLED, DISABLED Default value: DISABLED

dns64Timeout While doing DNS64 resolution, this parameter specifies the time to wait before sending an A query if no response is received from backend DNS server for AAAA query. Default value: -1 Maximum value: 10000

ecsMaxSubnets Maximum number of subnets that can be cached corresponding to a single domain. Subnet caching will occur for responses with EDNS Client Subnet (ECS) option. Caching of such responses can be disabled using DNS profile settings. A value of zero indicates that the number of subnets cached is limited only by existing memory constraints. The default value is zero. Default value: 0 Minimum value: 0 Maximum value: 1280

maxnegcacheTTL Maximum time to live (TTL) for all negative records (NXDONAIN and NODATA) cached in the DNS cache by DNS proxy, end resolver, and forwarder configurations. If the TTL of a record that is to be cached is higher than the value configured for maxnegcacheTTL, the TTL of the record is set to the value of maxnegcacheTTL before caching. When you modify this setting, the new value is applied only to those records that are cached after the modification. The TTL values of existing records are not changed. Default value: 604800 Minimum value: 1 Maximum value: 604800

cacheHitBypass This parameter is applicable only in proxy mode and if this parameter is enabled we will forward all the client requests to the backend DNS server and the response served will be cached on Citrix ADC

Possible values: ENABLED, DISABLED Default value: DISABLED

maxCacheSize Maximum memory, in megabytes, that can be used for dns caching per Packet Engine.

maxNegativeCacheSize Maximum memory, in megabytes, that can be used for caching of negative DNS responses per packet engine.

cacheNoExpire If this flag is set to YES, the existing entries in cache do not age out. On reaching the max limit the cache records are frozen

Possible values: ENABLED, DISABLED Default value: DISABLED

splitPktQueryProcessing Processing requests split across multiple packets

Possible values: ALLOW, DROP Default value: ALLOW

cacheECSZeroPrefix Cache ECS responses with a Scope Prefix length of zero. Such a cached response will be used for all queries with this domain name and any subnet. When disabled, ECS responses with Scope Prefix length of zero will be cached, but not tied to any subnet. This option has no effect if caching of ECS responses is disabled in the corresponding DNS profile.

Possible values: ENABLED, DISABLED Default value: ENABLED

maxUDPPacketSize Maximum UDP packet size that can be handled by Citrix ADC. This is the value advertised by Citrix ADC when responding as an authoritative server and it is also used when Citrix ADC queries other name servers as a forwarder. When acting as a proxy, requests from clients are limited by this parameter - if a request contains a size greater than this value in the OPT record, it will be replaced. Default value: 1280 Minimum value: 512 Maximum value: 16384

NXDomainRateLimitThreshold Rate limit threshold for Non-Existant domain (NXDOMAIN) responses generated from Citrix ADC. Once the threshold is breached , DNS queries leading to NXDOMAIN response will be dropped. This threshold will not be applied for NXDOMAIN responses got from the backend. The threshold will be applied per packet engine and per second. Minimum value: 0

dns-policy

The following operations can be performed on "dns-policy":

show| set| rm| add| unset|

show dns policy

Displays the parameters of the specified DNS policy or, if no policy name is specified, all configured DNS policies.

Synopsis

show dns policy

Arguments

name Name of the DNS policy.

Output

rule The expression to be used by the dns policy.

viewName The view name that must be used for the given policy

preferredLocation The location used for the given policy. This is deprecated attribute. Please use -prefLocList

preferredLocList The location list in priority order used for the given policy.

hits The number of times the policy has been hit.

undefHits Number of Undef hits.

drop The dns packet must be dropped.

actionName Name of the DNS action to perform when the rule evaluates to TRUE. The built in actions function as follows:

- dns_default_act_Drop. Drop the DNS request.
- dns_default_act_Cachebypass. Bypass the DNS cache and forward the request to the name server. You can create custom actions by using the add dns action command in the CLI or the DNS > Actions > Create DNS Action dialog box in the Citrix ADC configuration utility.

cacheBypass By pass dns cache for this.

activePolicy Indicates whether policy is bound or not.

boundTo Location where policy is bound

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

description Description of the policy

logAction Name of the messagelog action to use for requests that match this policy.

builtin Flag to determine whether DNS policy is default or not

feature The feature to be checked while applying this config

stateflag type devno count

set dns policy

Modifies the parameters of the specified DNS policy.

Synopsis

set dns policy <name>

Arguments

name Name of the DNS policy.

rule Expression against which DNS traffic is evaluated. Note:

- On the command line interface, if the expression includes blank spaces, the entire expression must be enclosed in double quotation marks.
- If the expression itself includes double quotation marks, you must escape the quotations by using the character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Example: CLIENT.UDP.DNS.DOMAIN.EQ("domainname")

actionName Name of the DNS action to perform when the rule evaluates to TRUE. The built in actions function as follows:

- dns_default_act_Drop. Drop the DNS request.

- dns_default_act_Cachebypass. Bypass the DNS cache and forward the request to the name server. You can create custom actions by using the add dns action command in the CLI or the DNS > Actions > Create DNS Action dialog box in the Citrix ADC configuration utility.

logAction Name of the messagelog action to use for requests that match this policy.

Example

set dns policy pol1 -rule "dns.req.question.type.ne(aaaa)" set dns policy pol2 -rule "CLIENT.IP.SRC.IN_SUBNET(1.1.1.1/24)" set dns policy pol1 -rule dns.res.header.rcode.eq(nxdomain)

rm dns policy

Removes a DNS policy.

Synopsis

rm dns policy <name>

Arguments

name Name of the DNS policy to remove.

add dns policy

Creates a DNS policy.

Synopsis

add dns policy <name> <rule>

Arguments

name Name for the DNS policy.

rule Expression against which DNS traffic is evaluated. Note:

- On the command line interface, if the expression includes blank spaces, the entire expression must be enclosed in double quotation marks.
- If the expression itself includes double quotation marks, you must escape the quotations by using the character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Example: CLIENT.UDP.DNS.DOMAIN.EQ("domainname")

actionName Name of the DNS action to perform when the rule evaluates to TRUE. The built in actions function as follows:

- dns_default_act_Drop. Drop the DNS request.
- dns_default_act_Cachebypass. Bypass the DNS cache and forward the request to the name server. You can create custom actions by using the add dns action command in the CLI or the DNS > Actions > Create DNS Action dialog box in the Citrix ADC configuration utility.

logAction Name of the messagelog action to use for requests that match this policy.

Example

add dns policy pol1 "dns.req.question.type.ne(aaaa)" -actionName act1 add dns policy pol2 "CLIENT.IP.SRC.IN_SUBNET(1.1.1.1/24)" -actionName action1 add dns policy pol1 dns.res.question.domain.contains("citrix") -actionName act2

unset dns policy

Use this command to remove dns policy settings.Refer to the set dns policy command for meanings of the arguments.

Synopsis

unset dns policy <name> -logAction

dns-policy64

The following operations can be performed on "dns-policy64":

rm| show| add| set|

rm dns policy64

Removes a DNS64 Policy.

Synopsis

rm dns policy64 <name>

Arguments

name Name of the DNS64 policy to be removed.

show dns policy64

Displays the parameters of the specified DNS64 policy or, if no policy name is specified, all configured DNS64 policies.

Synopsis

show dns policy64

Arguments

name Name of the DNS64 policy.

Output

rule The expression to be used by the dns policy.

hits The number of times the policy has been hit.

action Name of the DNS64 action to perform when the rule evaluates to TRUE. The built in actions function as follows:

- A default dns64 action with prefix <default prefix> and mapped and exclude are any You can create custom actions by using the add dns action command in the CLI or the DNS64 > Actions > Create DNS64 Action dialog box in the Citrix ADC configuration utility.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

boundTo Location where policy is bound

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

undefHits Number of Undef hits.

description Description of the policy

stateflag devno count

add dns policy64

Creates a DNS64 Policy.

Synopsis

add dns policy64 <name> -rule <expression> -action <string>

Arguments

name Name for the DNS64 policy.

rule Expression against which DNS traffic is evaluated. Note:

- On the command line interface, if the expression includes blank spaces, the entire expression must be enclosed in double quotation marks.
- If the expression itself includes double quotation marks, you must escape the quotations by using the character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Example: CLIENT.IP.SRC.IN_SUBENT(23.34.0.0/16)

action Name of the DNS64 action to perform when the rule evaluates to TRUE. The built in actions function as follows:

- A default dns64 action with prefix <default prefix> and mapped and exclude are any You can create custom actions by using the add dns action command in the CLI or the DNS64 > Actions > Create DNS64 Action dialog box in the Citrix ADC configuration utility.

Example

add dns64 policy pol1 "client.ip.src.in_subnet(23.43.0.0/16)" -action act1

set dns policy64

Modifies the parameters of the specified DNS64 policy.

Synopsis

set dns policy64 <name>

Arguments

name Name of the DNS policy.

rule Expression against which DNS traffic is evaluated. Note:

- On the command line interface, if the expression includes blank spaces, the entire expression must be enclosed in double quotation marks.

- If the expression itself includes double quotation marks, you must escape the quotations by using the character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Example: CLIENT.IP.SRC.IN_SUBENT(23.34.0.0/16)

action Name of the DNS64 action to perform when the rule evaluates to TRUE. The built in actions function as follows:

- A default dns64 action with prefix <default prefix> and mapped and exclude are any You can create custom actions by using the add dns action command in the CLI or the DNS64 > Actions > Create DNS64 Action dialog box in the Citrix ADC configuration utility.

Example

set dns policy pol2 -rule "CLIENT.IP.SRC.IN_SUBNET(1.1.1.1/24)"

dns-policylabel

The following operations can be performed on "dns-policylabel":

show| add| unbind| stat| rename| bind| rm|

show dns policylabel

Display policy label or policies bound to dns policylabel.

Synopsis

show dns policylabel

Arguments

labelName Name of the dns policy label.

Output

stateflag transform The type of transformations allowed by the policies bound to the label.

numpol Number of polices bound to label.

hits Number of times policy label was invoked.

policyName The dns policy name.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke Invoke flag.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

flowType Flowtype of the bound dns policy.

description Description of the policylabel

isDefault A value of true is returned if it is a default dns policylabel.

flags devno count

Example

i)show dns policylabel trans_dns ii)show dns policylabel

add dns policylabel

Add a dns policy label.

Synopsis

add dns policylabel <labelName> <transform>

Arguments

labelName Name of the dns policy label.

transform The type of transformations allowed by the policies bound to the label.

Possible values: dns_req, dns_res

Example

add dns policylabel trans_dns dns_req

unbind dns policylabel

Unbind entities from dns label.

Synopsis

unbind dns policylabel <labelName> <policyName>

Arguments

labelName Name of the dns policy label.

policyName The dns policy name.

priority Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind dns policylabel trans_dns pol_1

stat dns policylabel

Display statistics of dns policylabel(s).

Synopsis

stat dns policylabel

Arguments

labelName The name of the dns policy label for which statistics will be displayed. If not given statistics are shown for all dns policylabels.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy Label Hits (Hits) Number of times policy label was invoked.

Related Commands

- stat dns records

rename dns policylabel

Rename a dns policy label.

Synopsis

rename dns policylabel <labelName>@ <newName>@

Arguments

labelName The name of the dns policylabel.

newName The new name of the dns policylabel.

Example

rename dns policylabel oldname newname

bind dns policylabel

Bind the dns policy to one of the labels.

Synopsis

bind dns policylabel <labelName> <policyName> <priority>

Arguments

labelName Name of the dns policy label.

policyName The dns policy name.

priority Priority with which the policy is to be bound. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE. oIf gotoPriorityExpression is not present or if it is equal to END then the policy bank evaluation ends here oElse if the gotoPriorityExpression is equal to NEXT then the next policy in the priority order is evaluated. oElse gotoPriorityExpression

is evaluated. The result of gotoPriorityExpression (which has to be a number) is processed as follows: -An UNDEF event is triggered if .gotoPriorityExpression cannot be evaluated .gotoPriorityExpression evaluates to number which is smaller than the maximum priority in the policy bank but is not same as any policy's priority .gotoPriorityExpression evaluates to a priority that is smaller than the current policy's priority -If the gotoPriorityExpression evaluates to the priority of the current policy then the next policy in the priority order is evaluated. -If the gotoPriorityExpression evaluates to the priority of a policy further ahead in the list then that policy will be evaluated next.

invoke Invoke flag.

labelType Type of policy label invocation.

Possible values: policylabel

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

Example

i)bind dns policylabel trans_dns pol_1 1 2 -invoke reqvserver CURRENT ii)bind rewrite policylabel trans_http_url pol_2 2

rm dns policylabel

Remove a dns policy label.

Synopsis

rm dns policylabel <labelName>

Arguments

labelName Name of the dns policy label.

Example

rm dns policylabel trans_dns

dns-profile

The following operations can be performed on "dns-profile":

set| add| rm| unset| show|

set dns profile

Modifies the attributes of a DNS profile.

Synopsis

set dns profile <dnsProfileName>

Arguments

dnsProfileName Name of the DNS profile

dnsQueryLogging DNS query logging; if enabled, DNS query information such as DNS query id, DNS query flags , DNS domain name and DNS query type will be logged

Possible values: ENABLED, DISABLED Default value: DISABLED

dnsAnswerSecLogging DNS answer section; if enabled, answer section in the response will be logged.

Possible values: ENABLED, DISABLED Default value: DISABLED

dnsExtendedLogging DNS extended logging; if enabled, authority and additional section in the response will be logged.

Possible values: ENABLED, DISABLED Default value: DISABLED

dnsErrorLogging DNS error logging; if enabled, whenever error is encountered in DNS module reason for the error will be logged.

Possible values: ENABLED, DISABLED Default value: DISABLED

cacheRecords Cache resource records in the DNS cache. Applies to resource records obtained through proxy configurations only. End resolver and forwarder configurations always cache records in the DNS cache, and you cannot disable this behavior. When you disable record caching, the appliance stops caching server responses. However, cached records are not flushed. The appliance does not serve requests from the cache until record caching is enabled again.

Possible values: ENABLED, DISABLED Default value: ENABLED

cacheNegativeResponses Cache negative responses in the DNS cache. When disabled, the appliance stops caching negative responses except referral records. This applies to all configurations - proxy, end resolver, and forwarder. However, cached responses are not flushed.

The appliance does not serve negative responses from the cache until this parameter is enabled again.

Possible values: ENABLED, DISABLED Default value: ENABLED

dropMultiQueryRequest Drop the DNS requests containing multiple queries. When enabled, DNS requests containing multiple queries will be dropped. In case of proxy configuration by default the DNS request containing multiple queries is forwarded to the backend and in case of ADNS and Resolver configuration NOCODE error response will be sent to the client.

Possible values: ENABLED, DISABLED Default value: DISABLED

cacheECSResponses Cache DNS responses with EDNS Client Subnet(ECS) option in the DNS cache. When disabled, the appliance stops caching responses with ECS option. This is relevant to proxy configuration. Enabling/disabling support of ECS option when Citrix ADC is authoritative for a GSLB domain is supported using a knob in GSLB vserver. In all other modes, ECS option is ignored.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set dns profile <profile name> -caching ENABLED

add dns profile

Creates a DNS profile. These DNS profiles can be associated with DNS/DNS-TCP LB vservers ,ADNS/ADNS-TCP services , end resolvers and with DNS actions. DNS profiles dictate the caching and logging behavior for a DNS transaction.

Synopsis

add dns profile <dnsProfileName>

Arguments

dnsProfileName Name of the DNS profile

dnsQueryLogging DNS query logging; if enabled, DNS query information such as DNS query id, DNS query flags , DNS domain name and DNS query type will be logged

Possible values: ENABLED, DISABLED Default value: DISABLED

dnsAnswerSecLogging DNS answer section; if enabled, answer section in the response will be logged.

Possible values: ENABLED, DISABLED Default value: DISABLED

dnsExtendedLogging DNS extended logging; if enabled, authority and additional section in the response will be logged.

Possible values: ENABLED, DISABLED Default value: DISABLED

dnsErrorLogging DNS error logging; if enabled, whenever error is encountered in DNS module reason for the error will be logged.

Possible values: ENABLED, DISABLED Default value: DISABLED

cacheRecords Cache resource records in the DNS cache. Applies to resource records obtained through proxy configurations only. End resolver and forwarder configurations always cache records in the DNS cache, and you cannot disable this behavior. When you disable record caching, the appliance stops caching server responses. However, cached records are not flushed. The appliance does not serve requests from the cache until record caching is enabled again.

Possible values: ENABLED, DISABLED Default value: ENABLED

cacheNegativeResponses Cache negative responses in the DNS cache. When disabled, the appliance stops caching negative responses except referral records. This applies to all configurations - proxy, end resolver, and forwarder. However, cached responses are not flushed. The appliance does not serve negative responses from the cache until this parameter is enabled again.

Possible values: ENABLED, DISABLED Default value: ENABLED

dropMultiQueryRequest Drop the DNS requests containing multiple queries. When enabled, DNS requests containing multiple queries will be dropped. In case of proxy configuration by default the DNS request containing multiple queries is forwarded to the backend and in case of ADNS and Resolver configuration NOCODE error response will be sent to the client.

Possible values: ENABLED, DISABLED Default value: DISABLED

cacheECSResponses Cache DNS responses with EDNS Client Subnet(ECS) option in the DNS cache. When disabled, the appliance stops caching responses with ECS option. This is relevant to proxy configuration. Enabling/disabling support of ECS option when Citrix ADC is authoritative for a

GSLB domain is supported using a knob in GSLB vserver. In all other modes, ECS option is ignored.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

add dns profile testprofile -caching yes

rm dns profile

Removes the specified DNS profile from the Citrix ADC

Synopsis

rm dns profile <dnsProfileName>

Arguments

dnsProfileName Name of the DNS profile to be removed.

Example

rm dns profile testprofile

unset dns profile

Use this command to remove dns profile settings.Refer to the set dns profile command for meanings of the arguments.

Synopsis

unset dns profile <dnsProfileName>

show dns profile

Displays the properties of the specified DNS profile. If profile name is not specified then all conifgured DNS profiles are displayed

Synopsis

show dns profile

Arguments

dnsProfileName Name of the DNS profile

Output

dnsQueryLogging DNS query logging; if enabled, DNS query information such as DNS query id, DNS query flags , DNS domain name and DNS query type will be logged

dnsAnswerSecLogging DNS answer section; if enabled, answer section in the response will be logged.

dnsExtendedLogging DNS extended logging; if enabled, authority and additional section in the response will be logged.

dnsErrorLogging DNS error logging; if enabled, whenever error is encountered in DNS module reason for the error will be logged.

cacheRecords Cache resource records in the DNS cache. Applies to resource records obtained through proxy configurations only. End resolver and forwarder configurations always cache records in the DNS cache, and you cannot disable this behavior. When you disable record caching, the appliance stops caching server responses. However, cached records are not flushed. The appliance does not serve requests from the cache until record caching is enabled again.

cacheNegativeResponses Cache negative responses in the DNS cache. When disabled, the appliance stops caching negative responses except referral records. This applies to all configurations - proxy, end resolver, and forwarder. However, cached responses are not flushed. The appliance does not serve negative responses from the cache until this parameter is enabled again.

dropMultiQueryRequest Drop the DNS requests containing multiple queries. When enabled, DNS requests containing multiple queries will be dropped. In case of proxy configuration by default the DNS request containing multiple queries is forwarded to the backend and in case of ADNS and Resolver configuration NOCODE error response will be sent to the client.

cacheECSResponses Cache DNS responses with EDNS Client Subnet(ECS) option in the DNS cache. When disabled, the appliance stops caching responses with ECS option. This is relevant to proxy configuration. Enabling/disabling support of ECS option when Citrix ADC is authoritative for a GSLB domain is supported using a knob in GSLB vserver. In all other modes, ECS option is ignored.

referenceCount Number of entities using this profile

devno count stateflag

Example

show dns profile

dns-proxyRecords

The following operations can be performed on "dns-proxyRecords":

flush dns proxyRecords

Flushes all/selected (via -type or -negRecType) proxy records from the DNS cache on the Citrix ADC.

Synopsis

flush dns proxyRecords (-type <type> | -negRecType (NXDOMAIN | NODATA))

Arguments

type Filter the DNS records to be flushed.e.g flush dns proxyRecords -type A will flush only the A records from the cache.

Possible values: A, NS, CNAME, SOA, MX, AAAA, SRV, RRSIG, NSEC, DNSKEY, PTR, TXT, NAPTR, CAA

negRecType Filter the Negative DNS records i.e NXDOMAIN and NODATA entries to be flushed. e.g flush dns proxyRecords NXDOMAIN will flush only the NXDOMAIN entries from the cache

Possible values: NXDOMAIN, NODATA

dns-ptrRec

The following operations can be performed on "dns-ptrRec":

add| rm| show|

add dns ptrRec

Creates a pointer (PTR) record for the specified reverse domain name.

Synopsis

add dns ptrRec <reverseDomain> <domain> ...

Arguments

reverseDomain Reversed domain name representation of the IPv4 or IPv6 address for which to create the PTR record. Use the "in-addr.arpa." suffix for IPv4 addresses and the "ip6.arpa." suffix for IPv6 addresses.

domain Domain name for which to configure reverse mapping.

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

Example

add dns ptrrec 1.1.1.in-addr.arpa. abc.com

rm dns ptrRec

Removes a pointer (PTR) record for the specified domain name and reverse domain name. For EDNS Client Subnet (ECS) records, a subnet needs to be specified to remove a PTR record for the specified domain name and reverse domain name which is cached for that particular subnet

Synopsis

rm dns ptrRec <reverseDomain> [-ecsSubnet <ip_addr|ipv6_addr>]

Arguments

reverseDomain Reverse domain name of the PTR record.

ecsSubnet Subnet for which the cached PTR record need to be removed.

domain Domain name for which to remove reverse mapping.

Example

rm dns ptrrec 1.1.1.1.in-addr.arpa. ptr.com

show dns ptrRec

Displays the pointer (PTR) record for the specified reverse domain name and domain name.

Synopsis

show dns ptrRec

Arguments

reverseDomain Reversed domain name representation of the IPv4 or IPv6 address for which to create the PTR record. Use the "in-addr.arpa." suffix for IPv4 addresses and the "ip6.arpa." suffix for IPv6 addresses.

type Type of records to display. Available settings function as follows:

- ADNS - Display all authoritative address records.
- PROXY - Display all proxy address records.
- ALL - Display all address records.

Possible values: ALL, ADNS, PROXY

Output

domain Domain name for which to configure reverse mapping.

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600.

authType Authentication type.

ecsSubnet Subnet for which this particular record is cached. Subnet caching will occur for responses with EDNS Client Subnet (ECS) option. Applies to resource records obtained through proxy configurations only.

devno count stateflag

dns-records

The following operations can be performed on "dns-records":

stat dns records

Displays statistics for the specified DNS record or query type. If a DNS record or query type is not specified, statistics for all record and query types are shown.

Synopsis

stat dns records

Arguments

dnsRecordType Display statistics for the specified DNS record or query type or, if a record or query type is not specified, statistics for all record types supported on the Citrix ADC.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Total entries (totEntries) Total number of DNS record entries

Total updates (totUpdates) Total number of DNS proactive updates

Total responses (totResp) Total number of DNS server responses

Total requests (totReq) Total number of DNS queries recieved

Current entries (curEnt) Current number of DNS entries

Total Query for Expired Record (totQueryForExpiredRecord) Total number of times query was received for expired record

Total limit errors (errLim) Total number of times we have recieved dns record with more entries than we support

Total response format errors (errRespFor) Total number of times we have recieved malformed responses from the backend

Total alias exist errors (errAlias) Total number of times we have recieved non-cname record for a domain for which an alias exists

Total cache misses (errNoDom) Total number of cache misses

Current records (curRec) Current number of DNS Records

Related Commands

- stat dns policylabel

dns-soaRec

The following operations can be performed on "dns-soaRec":

unset| show| rm| add| set|

unset dns soaRec

Use this command to remove dns soaRec settings.Refer to the set dns soaRec command for meanings of the arguments.

Synopsis

unset dns soaRec <domain>

show dns soaRec

Displays the parameters of the specified Start of Authority (SOA) record. If no domain name is specified, all SOA records are displayed.

Synopsis

show dns soaRec

Arguments

domain The domain name.

type Type of records to display. Available settings function as follows:

- ADNS - Display all authoritative address records.
- PROXY - Display all proxy address records.
- ALL - Display all address records.

Possible values: ALL, ADNS, PROXY

Output

originServer Domain name of the name server that responds authoritatively for the domain.

contact Email address of the contact to whom domain issues can be addressed. In the email address, replace the @ sign with a period (.). For example, enter domainadmin.example.com instead of domainadmin@example.com.

serial The secondary server uses this parameter to determine whether it requires a zone transfer from the primary server.

refresh Time, in seconds, for which a secondary server must wait between successive checks on the value of the serial number.

retry Time, in seconds, between retries if a secondary server's attempt to contact the primary server for a zone refresh fails.

expire Time, in seconds, after which the zone data on a secondary name server can no longer be considered authoritative because all refresh and retry attempts made during the period have failed. After the expiry period, the secondary server stops serving the zone. Typically one week. Not used by the primary server.

minimum Default time to live (TTL) for all records in the zone. Can be overridden for individual records.

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600.

authType Record type.

ecsSubnet Subnet for which this particular record is cached. Subnet caching will occur for responses with EDNS Client Subnet (ECS) option. Applies to resource records obtained through proxy configurations only.

devno count stateflag

rm dns soaRec

Removes the Start of Authority (SOA) record for the specified domain name. For EDNS Client Subnet (ECS) records, a subnet needs to be specified to remove the SOA record which is cached for that particular subnet

Synopsis

rm dns soaRec <domain> [-ecsSubnet <ip_addr|ipv6_addr>]

Arguments

domain Domain name of the SOA record.

ecsSubnet Subnet for which the cached SOA record need to be removed.

add dns soaRec

Creates a Start of Authority (SOA) record. Note: You can set the SOA parameters that are associated with zone transfers. However, the Citrix ADC currently does not support zone transfers.

Synopsis

add dns soaRec <domain> -originServer <string> -contact <string>

Arguments

domain Domain name for which to add the SOA record.

originServer Domain name of the name server that responds authoritatively for the domain.

contact Email address of the contact to whom domain issues can be addressed. In the email address, replace the @ sign with a period (.). For example, enter domainadmin.example.com instead of domainadmin@example.com.

serial The secondary server uses this parameter to determine whether it requires a zone transfer from the primary server. Default value: 100 Minimum value: 0 Maximum value: 4294967294

refresh Time, in seconds, for which a secondary server must wait between successive checks on the value of the serial number. Default value: 3600 Maximum value: 4294967294

retry Time, in seconds, between retries if a secondary server's attempt to contact the primary server for a zone refresh fails. Default value: 3 Maximum value: 4294967294

expire Time, in seconds, after which the zone data on a secondary name server can no longer be considered authoritative because all refresh and retry attempts made during the period have failed. After the expiry period, the secondary server stops serving the zone. Typically one week. Not used by the primary server. Default value: 3600 Maximum value: 4294967294

minimum Default time to live (TTL) for all records in the zone. Can be overridden for individual records. Default value: 5 Maximum value: 2147483647

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

set dns soaRec

Modifies the parameters of the specified Start Of Authority (SOA) record.

Synopsis

set dns soaRec <domain>

Arguments

domain Domain of the SOA record to be modified.

originServer Domain name of the name server that responds authoritatively for the domain.

contact Email address of the contact to whom domain issues can be addressed. In the email address, replace the @ sign with a period (.). For example, enter domainadmin.example.com instead of domainadmin@example.com.

serial The secondary server uses this parameter to determine whether it requires a zone transfer from the primary server. Default value: 100 Minimum value: 1 Maximum value: 4294967294

refresh Time, in seconds, for which a secondary server must wait between successive checks on the value of the serial number. Default value: 3600 Maximum value: 4294967294

retry Time, in seconds, between retries if a secondary server's attempt to contact the primary server for a zone refresh fails. Default value: 3 Maximum value: 4294967294

expire Time, in seconds, after which the zone data on a secondary name server can no longer be considered authoritative because all refresh and retry attempts made during the period have failed. After the expiry period, the secondary server stops serving the zone. Typically one week. Not used by the primary server. Default value: 3600 Maximum value: 4294967294

minimum Default time to live (TTL) for all records in the zone. Can be overridden for individual records. Default value: 5 Maximum value: 2147483647

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

dns-srvRec

The following operations can be performed on "dns-srvRec":

rm| show| set| unset| add|

rm dns srvRec

Removes, from the specified domain, the SRV record created for the service provided by the specified target host. For EDNS Client Subnet (ECS) records, a subnet needsto be specified to remove the SRV record created for the service provided by the specified target host which is cached for that particular subnet

Synopsis

rm dns srvRec <domain> <target> ... [-ecsSubnet <ip_addr|ipv6_addr>]

Arguments

domain Domain name of the SRV record.

target Target host for the specified service.

ecsSubnet Subnet for which the cached SRV record need to be removed.

show dns srvRec

Displays the service (SRV) record configured for the specified target host and domain. If the domain name is not specified, all of the SRV records are shown.

Synopsis

show dns srvRec [(<domain>) | -type <type>]

Arguments

domain Domain name for which to display the SRV record.

target Target host for the specified service.

type Type of records to display. Available settings function as follows:

- ADNS - Display all authoritative address records.
- PROXY - Display all proxy address records.
- ALL - Display all address records.

Possible values: ALL, ADNS, PROXY

Output

priority Priority of the target host. This helps in server selection by the client.

weight Weight for the target host. Aids host selection when two or more hosts have the same priority. A larger number indicates greater weight.

port Port on which the target host listens for client requests.

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600.

authType Record type.

ecsSubnet Subnet for which this particular record is cached. Subnet caching will occur for responses with EDNS Client Subnet (ECS) option. Applies to resource records obtained through proxy configurations only.

devno count stateflag

set dns srvRec

Modifies the parameters of the specified service (SRV) record.

Synopsis

set dns srvRec <domain> <target>

Arguments

domain Name of the SRV record to be modified.

target Target of the SRV record to be modified.

priority Integer specifying the priority of the target host. The lower the number, the higher the priority. If multiple target hosts have the same priority, selection is based on the Weight parameter. Minimum value: 0 Maximum value: 65535

weight Weight for the target host. Aids host selection when two or more hosts have the same priority. A larger number indicates greater weight. Minimum value: 0 Maximum value: 65535

port Port on which the target host listens for client requests. Minimum value: 0 Maximum value: 65535

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

unset dns srvRec

Use this command to remove dns srvRec settings.Refer to the set dns srvRec command for meanings of the arguments.

Synopsis

unset dns srvRec <domain> <target> -TTL

add dns srvRec

Creates a service (SRV) record for the service offered by the specified target host, in the specified domain.

Synopsis

add dns srvRec <domain> <target> -priority <positive_integer> -weight <positive_integer> -port <positive_integer>

Arguments

domain Domain name, which, by convention, is prefixed by the symbolic name of the desired service and the symbolic name of the desired protocol, each with an underscore (_) prepended. For example, if an SRV-aware client wants to discover a SIP service that is provided over UDP, in the domain example.com, the client performs a lookup for _sip._udp.example.com.

target Target host for the specified service.

priority Integer specifying the priority of the target host. The lower the number, the higher the priority. If multiple target hosts have the same priority, selection is based on the Weight parameter. Minimum value: 0 Maximum value: 65535

weight Weight for the target host. Aids host selection when two or more hosts have the same priority. A larger number indicates greater weight. Minimum value: 0 Maximum value: 65535

port Port on which the target host listens for client requests. Minimum value: 0 Maximum value: 65535

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

dns-stats

The following operations can be performed on "dns-stats":

show dns stats

show dns stats is an alias for stat dns

Synopsis

show dns stats - alias for 'stat dns'

dns-subnetcache

The following operations can be performed on "dns-subnetcache":

show| flush|

show dns subnetcache

Displays all the domains for which ECS records are cached for the given ECS subnet. It also displays the type of dns records cached for every domain associated with the subnet. If a subnet is not specified, all the configured ECS subnets on the Citrix ADC are shown.

Synopsis

show dns subnetcache

Arguments

ecsSubnet ECS Subnet.

Output

hostName Domain name.

nextRecs An array of record types associated with the domain name.

devno count stateflag

flush dns subnetcache

FLushes a specified ECS subnet or all cached ECS subnets from the DNS cache on the Citrix ADC.

Synopsis

flush dns subnetcache (<ecsSubnet> | -all)

Arguments

ecsSubnet ECS Subnet.

all Flush all the ECS subnets from the DNS cache.

dns-suffix

The following operations can be performed on "dns-suffix":

add| rm| show|

add dns suffix

Specifies a suffix that can be used to complete domain names that are not fully qualified. For example, if you specify the example.com suffix, and the Citrix ADC is required to resolve the incomplete domain name "myhost," it attempts to resolve "myhost.example.com."

Synopsis

add dns suffix <dnsSuffix>

Arguments

dnsSuffix Suffix to be appended when resolving domain names that are not fully qualified.

Example

add dns suffix netscaler.com

If the incoming domain name "engineering" is not resolved by itself, the system will append the suffix netscaler.com and attempt to resolve the name engineering.netscaler.com.

rm dns suffix

Removes a DNS suffix.

Synopsis

rm dns suffix <dnsSuffix>

Arguments

dnsSuffix DNS suffix to remove.

show dns suffix

Displays the specified DNS suffix or, if no DNS suffix is specified, all configured DNS suffixes.

Synopsis

show dns suffix

Arguments

dnsSuffix DNS suffix to display.

Output

devno count stateflag

dns-txtRec

The following operations can be performed on "dns-txtRec":

show| rm| add|

show dns txtRec

Displays TXT records owned by the specified domain. If no domain name is specified, all configured TXT records are shown.

Synopsis

show dns txtRec

Arguments

domain Name of the domain for the TXT record.

type Type of records to display. Available settings function as follows:

- ADNS - Display all authoritative address records.
- PROXY - Display all proxy address records.
- ALL - Display all address records.

Possible values: ALL, ADNS, PROXY Default value: ADNS

Output

string Information to store in the TXT resource record. Enclose the string in single or double quotation marks. A TXT resource record can contain up to six strings, each of which can contain up to 255 characters. If you want to add a string of more than 255 characters, evaluate whether splitting it into two or more smaller strings, subject to the six-string limit, works for you.

ecsSubnet Subnet for which this particular record is cached. Subnet caching will occur for responses with EDNS Client Subnet (ECS) option. Applies to resource records obtained through proxy configurations only

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600.

recordId authType Authentication type.

devno count stateflag

Example

show dns txtRec spf.m.test. show dns txtRec

rm dns txtRec

Removes the specified TXT record from the specified domain. For EDNS Client Subnet (ECS) records, a subnet needs to be specified to remove a TXT record which is cached for that particular subnet.

Synopsis

rm dns txtRec <domain> (<string> ... | -recordId <positive_integer>@) [-ecsSubnet <ip_addr|ipv6_addr>]

Arguments

domain Name of the domain for the TXT record.

string Complete set of text strings in the TXT record, entered in the order in which they are stored in the record. Mutually exclusive with the record ID parameter.

recordId Unique, internally generated record ID. View the details of the TXT record to obtain its record ID. Mutually exclusive with the string parameter. Minimum value: 1 Maximum value: 65535

ecsSubnet Subnet for which the cached TXT record need to be removed.

Example

rm dns txtRec spf.m.test. "v=spf1 ip4:1.2.3.0/24 ip4:1.3.4.0/24 ?all" rm dns txtRec comments.m.test. "This is a CHARSTR" "This is another CHARSTR" rm dns txtRec comments.m.test. -recordId 1411

add dns txtRec

Creates a text (TXT) record for the specified domain name. Each resource record is stored with a unique, internally generated record ID, which you can view and use to delete the record. You cannot modify a TXT resource record.

Synopsis

add dns txtRec <domain> <string> ...

Arguments

domain Name of the domain for the TXT record.

string Information to store in the TXT resource record. Enclose the string in single or double quotation marks. A TXT resource record can contain up to six strings, each of which can contain up to 255 characters. If you want to add a string of more than 255 characters, evaluate whether splitting it into two or more smaller strings, subject to the six-string limit, works for you.

TTL Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Maximum value: 2147483647

Example

add dns txtRec spf.m.test. "v=spf1 ip4:1.2.3.0/24 ip4:1.3.4.0/24 ?all" add dns txtRec comments.m.test. "This is a CHARSTR" "This is another CHARSTR"

dns-view

The following operations can be performed on "dns-view":

add| rm| show|

add dns view

Creates a DNS view. A DNS view is used in global server load balancing (GSLB) to return a predetermined IP address to a specific group of clients, which are identified by using a DNS policy.

Synopsis

add dns view <viewName>

Arguments

viewName Name for the DNS view.

Example

add dns view privateview

rm dns view

Removes a DNS view.

Synopsis

rm dns view <viewName>

Arguments

viewName Name for the DNS view.

Example

rm dns view privateview

show dns view

Displays the specified DNS view or, if no DNS view name is specified, all the DNS views configured on the Citrix ADC.

Synopsis

show dns view

Arguments

viewName Name of the view to display.

Output

serviceName Service name of the service using this view.

gslbServiceName Service name of the service using this view.

dnsPolicyName dnspolicy name of this view.

IPAddress IP of the service corresponding to the given view.

flags Flags controlling display.

stateflag flags controlling display

devno count

dns-zone

The following operations can be performed on "dns-zone":

rm| add| sign| show| unset| unsign| set|

rm dns zone

Removes a DNS zone from the Citrix ADC.

Synopsis

rm dns zone <zoneName>

Arguments

zoneName Name of the zone to remove.

add dns zone

Creates a DNS zone on the Citrix ADC. Mandatory if you want to use the appliance to implement Domain Name Security Extensions (DNSSEC) for the zone. When you add a DNS resource record, if the domain name of the record belongs to the zone, the record is automatically added to the zone.

Synopsis

add dns zone <zoneName> -proxyMode (YES | NO) [-dnssecOffload (ENABLED | DISABLED)]

Arguments

zoneName Name of the zone to create.

proxyMode Deploy the zone in proxy mode. Enable in the following scenarios:

- The load balanced DNS servers are authoritative for the zone and all resource records that are part of the zone.
- The load balanced DNS servers are authoritative for the zone, but the Citrix ADC owns a subset of the resource records that belong to the zone (partial zone ownership configuration). Typically seen in global server load balancing (GSLB) configurations, in which the appliance responds authoritatively to queries for GSLB domain names but forwards queries for other domain names in the zone to the load balanced servers. In either scenario, do not create the zone's Start of Authority (SOA) and name server (NS) resource records on the appliance. Disable if the appliance is authoritative for the zone, but make sure that you have created the SOA and NS records on the appliance before you create the zone.

Possible values: YES, NO Default value: ENABLED

dnssecOffload Enable dnssec offload for this zone.

Possible values: ENABLED, DISABLED Default value: DISABLED

nsec Enable nsec generation for dnssec offload.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

add dns zone foo.bar -proxyMode NO -dnssec ENABLED

sign dns zone

Signs a DNS zone with a DNS key. Before you sign a zone, make sure that you've enabled DNSSEC by setting the global DNS parameter "Enable DNSSEC extension."

Synopsis

sign dns zone <zoneName>

Arguments

zoneName Name of the zone.

keyName Name of the public/private DNS key pair with which to sign the zone. You can sign a zone with up to four keys.

Example

sign dns zone abc.com. -keyname abc.com.zsk abc.com.ksk

show dns zone

Displays the parameters of the specified DNS zone, along with information about the types of resource records available for each domain name in the zone. If no zone name is specified, just the parameters are shown, for all configured zones.

Synopsis

show dns zone

Arguments

zoneName Name of the zone. Mutually exclusive with the type parameter.

type Type of zone to display. Mutually exclusive with the DNS Zone (zoneName) parameter. Available settings function as follows:

- ADNS - Display all the zones for which the Citrix ADC is authoritative.
- PROXY - Display all the zones for which the Citrix ADC is functioning as a proxy server.
- ALL - Display all the zones configured on the appliance.

Possible values: ALL, ADNS, PROXY

Output

proxyMode Deploy the zone in proxy mode. Enable in the following scenarios:

- The load balanced DNS servers are authoritative for the zone and all resource records that are part of the zone.
- The load balanced DNS servers are authoritative for the zone, but the Citrix ADC owns a subset of the resource records that belong to the zone (partial zone ownership configuration). Typically seen in global server load balancing (GSLB) configurations, in which the appliance responds authoritatively to queries for GSLB domain names but forwards queries for other

domain names in the zone to the load balanced servers. In either scenario, do not create the zone's Start of Authority (SOA) and name server (NS) resource records on the appliance. Disable if the appliance is authoritative for the zone, but make sure that you have created the SOA and NS records on the appliance before you create the zone.

flags Flags controlling display.

nsecBitarray Bit array representing the different record types configured for the domain name

domain Domain name that belongs to the given zone

nextRecs An array of record types associated with the nsec record.

stateflag flags controlling display

dnssecOffload Enable dnssec offload for this zone.

nsec Enable nsec generation for dnssec offload.

keyName Name of the public/private DNS key pair with which to sign the zone. You can sign a zone with up to four keys.

sigInceptionTime The time when sign was done with this key.

signed Integer which denote status of keys.

expires Time period for which to consider the key valid, after the key is used to sign a zone.

devno count

Example

show dns zone foo.bar

unset dns zone

Use this command to remove dns zone settings.Refer to the set dns zone command for meanings of the arguments.

Synopsis

unset dns zone <zoneName>

unsign dns zone

Unsigns the specified DNS zone with the specified DNS key.

Synopsis

unsign dns zone <zoneName>

Arguments

zoneName Name of the zone.

keyName Name of the public-private DNS key pair with which to unsign the zone.

Example

unsign dns zone abc.com. -keyname abc.com.zsk abc.com.ksk

set dns zone

Modifies the parameters of the specified DNS zone.

Synopsis

set dns zone <zoneName>

Arguments

zoneName Name of the zone.

proxyMode Deploy the zone in proxy mode. Enable in the following scenarios:

- The load balanced DNS servers are authoritative for the zone and all resource records that are part of the zone.
- The load balanced DNS servers are authoritative for the zone, but the Citrix ADC owns a subset of the resource records that belong to the zone (partial zone ownership configuration). Typically seen in global server load balancing (GSLB) configurations, in which the appliance responds authoritatively to queries for GSLB domain names but forwards queries for other domain names in the zone to the load balanced servers. In either scenario, do not create the zone's Start of Authority (SOA) and name server (NS) resource records on the appliance. Disable if the appliance is authoritative for the zone, but make sure that you have created the SOA and NS records on the appliance before you create the zone.

Possible values: YES, NO Default value: ENABLED

dnssecOffload Enable dnssec offload for this zone.

Possible values: ENABLED, DISABLED Default value: DISABLED

nsec Enable nsec generation for dnssec offload.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set dns zone foo.bar -proxyMode NO -dnssec ENABLED

dns

The following operations can be performed on "dns":

stat dns

Displays DNS statistics.

Synopsis

stat dns

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Dns queries (Q) Total number of DNS queries received.

Multi queries (MtQ) Total number of Multi Query request received.

Dns responses (Rsp) Total number of DNS responses received.

Server responses (SvrRsp) Total number of Server responses received.

Total Record updates (TotRecUp) Total number of record updates.

Current cache size (CurCacheSize) Current DNS cache size

Negative cache size (CurNegCacheSize) Current Negative DNS cache size

Dns UDP Jumbo queries (JumboQ) Total number of Jumbo DNS queries received over UDP.

Dns UDP Jumbo responses sent (JumboRsp) Total number of Jumbo DNS responses sent over UDP.

Dns UDP Jumbo responses received (JumboSvrRsp) Total number of Jumbo DNS responses received over UDP.

Auth answers (AuthAns) Number of queries which were authoritatively answered.

Server queries (SvrQ) Total number of Server queries sent.

Cache flush called (CaFsh) Total number of times cache was flushed.

Cache entries flushed (CaEntFsh) Total number of cache entries flushed.

Non-authoritative entries (PxyEnt) Total number of non-authoritative entries.

Authoritative entries (AthEnt) Total number of authoritative entries.

Nonexistent domain (NoDomain) Number of queries for which no record was found.

Response class unsupported (RspClsEr) Total number of responses for which response types were unsupported.

Invalid query format (InQFmt) Total number of queries whose format was invalid.

Stray answers (StryRsp) Total number of stray answers.

Incorrect RD length (BadRDlen) Number of DNS responses received with invalid resoure data length.

Requests refused (ReqRefused) Number of DNS requests refused.

NULL Attack (NullAttack) Total number of queries received where all the counts are 0.

Response type unsupported (RspNoSup) Total number of responses for which response type requested was unsupported.

Query class unsupported (QClsEr) Total number of queries for which query class was unsupported.

Invalid response format (InRspFmt) Total number of responses for which there was a format error.

No answer responses (NoAnswer) Number of DNS responses received without answer.

Multi queries disabled (MtQErr) Total number of times a multi query was disabled and received a multi query.

Other errors (OtherErr) Total number of other errors.

DNS64 queries Total number of DNS64 queries recieved.

DNS64 answers Total number of DNS64 answers served.

DNS64 rewrite answers Total number of DNS64 answers served after rewriting the response.

DNS64 responses Total number of responses recieved from backend in DNS64 context.

DNS64 GSLB Queries Total number of DNS64 queries for GSLB domain

DNS64 GSLB Answers Total number of DNS64 queries served.

DNS64 Total truncated answers Total number of Answers served with TC bit set in DNS64 context.

DNS64 Total A queries to server Total number of Queries sent by DNS64 module to backend.

DNS64 Total times AAAA query bypassed Total number of times AAAA query has been bypassed in DNS64 trnsaction.

DNS64 Total TCP queries Total number of dns64 queries over TCP

DNS64 Total Active policies Total number of active dns64 policies

DNS64 Total NODATA Responses Total number of responses recieved from backend with ancount 0

NS queries (NSQ) Total number of NS queries received.

SOA queries (SOAQ) Total number of SOA queries received.

PTR queries (PTRQ) Total number of PTR queries received.

SRV queries (SRVQ) Total number of SRV queries received.

A responses (ARsp) Total number of A responses received.

CNAME responses (CNRsp) Total number of CNAME responses received.

MX responses (MXRsp) Total number of MX responses received.

ANY responses (ANYRsp) Total number of ANY responses received.

NS updates (NSUp) Total number of NS record updates.

SOA updates (SOAUp) Total number of SOA record updates.

PTR updates (PTRUp) Total number of PTR record updates.

SRV updates (SRVUp) Total number of SRV record updates.

AAAA queries (AAAAQ) Total number of AAAA queries received.

A queries (AQ) Total number of A queries received.

CNAME queries (CNQ) Total number of CNAME queries received.

MX queries (MXQ) Total number of MX queries received.

ANY queries (ANYQ) Total number of ANY queries received.

AAAA responses (AAAARsp) Total number of AAAA responses received.

NS responses (NSRsp) Total number of NS responses received.

SOA responses (SOARsp) Total number of SOA responses received.

PTR responses (PTRRsp) Total number of PTR responses received.

SRV responses (SRVRsp) Total number of SRV responses received.

AAAA updates (AAAAUp) Total number of AAAA record updates.

A updates (AUp) Total number of A record updates.

MX updates (MXUp) Total number of MX record updates.

CNAME updates (CNUp) Total number of CNAME record updates.

AAAA records (AAAARec) Total number of AAAA records.

A records (ARec) Total number of A records.

MX records (MXRec) Total number of MX records.

CNAME records (CNRec) Total number of CNAME records.

NS records (NSRec) Total number of NS records.

SOA records (SOARec) Total number of SOA records.

PTR records (PTRRec) Total number of PTR records.

SRV records (SRVRec) Total number of SRV records.

No AAAA records (NoAAAARec) Total number of times AAAA record lookup failed.

No A records (NoARec) Total number of times A record lookup failed.

No MX records (NoMXRec) Total number of times MX record lookup failed.

No PTR records (NoPTRRec) Total number of times PTR record lookup failed.

No NS records (NoNSRec) Total number of times NS record lookup failed.

No CNAME records (NoCNRec) Total number of times CNAME record lookup failed.

No SOA records (NoSOARec) Total number of times SOA record lookup failed.

No SRV records (NoSRVRec) Total number of times SRV record lookup failed.

No ANY records (NoANYrec) Total number of times ANY query lookup failed.

Unsupported queries (NotSupQ) Total number of requests for which query type requested was unsupported.

Related Commands

- stat dns policylabel

endpoint

Endpoint

The entities on which you can perform NetScaler CLI operations:

- endpoint-info

endpoint-info

The following operations can be performed on "endpoint-info":

set| show| add| unset| rm| clear|

set endpoint info

Attaches multiple labels to existing endpoint, creates it otherwise

Synopsis

set endpoint info <endpointName>

Arguments

endpointKind Endpoint kind. Currently, IP endpoints are supported

Possible values: IP Default value: IP

endpointName Name of endpoint, depends on kind. For IP Endpoint - IP address.

endpointMetadata String of qualifiers, in dotted notation, structured metadata for an endpoint. Each qualifier is more specific than the one that precedes it, as in cluster.namespace.service. For example: cluster.default.frontend. Note: A qualifier that includes a dot (.) or space ( ) must be enclosed in double quotation marks.

endpointLabelsJson String representing labels in json form. Maximum length 16K

show endpoint info

API to get information of added IP endpoints

Synopsis

show endpoint info

Arguments

endpointKind Endpoint kind. Currently, IP endpoints are supported

Possible values: IP Default value: IP

endpointName Name of endpoint, depends on kind. For IP Endpoint - IP address.

Output

endpointMetadata String of qualifiers, in dotted notation, structured metadata for an endpoint. Each qualifier is more specific than the one that precedes it, as in cluster.namespace.service. For example: cluster.default.frontend. Note: A qualifier that includes a dot (.) or space ( ) must be enclosed in double quotation marks.

endpointLabelsJson String representing labels in json form. Maximum length 16K

devno count stateflag

add endpoint info

Attaches multiple labels to existing endpoint, creates it otherwise

Synopsis

add endpoint info <endpointName>

Arguments

endpointKind Endpoint kind. Currently, IP endpoints are supported

Possible values: IP Default value: IP

endpointName Name of endpoint, depends on kind. For IP Endpoint - IP address.

endpointMetadata String of qualifiers, in dotted notation, structured metadata for an endpoint. Each qualifier is more specific than the one that precedes it, as in cluster.namespace.service. For example: cluster.default.frontend. Note: A qualifier that includes a dot (.) or space ( ) must be enclosed in double quotation marks.

endpointLabelsJson String representing labels in json form. Maximum length 16K

unset endpoint info

Use this command to remove endpoint info settings.Refer to the set endpoint info command for meanings of the arguments.

Synopsis

unset endpoint info <endpointName>

rm endpoint info

Deletes endpoint labels or endpoint incase of IP type.

Synopsis

rm endpoint info <endpointName>

Arguments

endpointKind Endpoint kind. Currently, IP endpoints are supported

Possible values: IP Default value: IP

endpointName Name of endpoint, depends on kind. For IP Endpoint - IP address.

clear endpoint info

API to clear all endpoint information

Synopsis

clear endpoint info

Arguments

endpointKind Endpoint kind. Currently, IP endpoints are supported

Possible values: IP Default value: IP

feo

feo-action

The following operations can be performed on "feo-action":

unset| rm| show| add| set|

unset feo action

Modify a front end optimization action..Refer to the set feo action command for meanings of the arguments.

Synopsis

unset feo action <name>

rm feo action

Remove the specified front end optimization action.

Synopsis

rm feo action <name>

Arguments

name The name of the front end optimization action.

show feo action

Display the front end optimization actions defined, including the built-in actions.

Synopsis

show feo action

Arguments

name The name of the front end optimization action.

Output

stateflag pageExtendCache Extend the time period during which the browser can use the cached resource.

cacheMaxage Maxage for cache extension.

imgShrinkToAttrib Shrink image dimensions as per the height and width attributes specified in the



add feo action

Create a front end optimization action.

SYNOPSIS

add feo action <name>

ARGUMENTS

name The name of the front end optimization action.

pageExtendCache Extend the time period during which the browser can use the cached resource.

cacheMaxage Maxage for cache extension. Default value: 30 Minimum value: 0 Maximum value: 360

imgShrinkToAttrib Shrink image dimensions as per the height and width attributes specified in the



SET FEO ACTION

Modify a front end optimization action.
Synopsis
set feo action <name>
Arguments
name The name of the front end optimization action.

pageExtendCache Extend the time period during which the browser can use the cached resource.

cacheMaxage Maxage for cache extension. Default value: 30 Minimum value: 0 Maximum value: 360

imgShrinkToAttrib Shrink image dimensions as per the height and width attributes specified in the



Feo

The entities on which you can perform NetScaler CLI operations:

- feo-action
- feo
- feo-global
- feo-parameter
- feo-policy
- feo-stats

feo-global

The following operations can be performed on "feo-global":

unbind| bind| show|

unbind feo global

Unbind a front end optimization policy globally.

Synopsis

unbind feo global <policyName> [-type <type>]

Arguments

policyName Name of the front end optimization policy.

type Bindpoint, specifying from where to unbind the policy. Applicable only to advanced (default-syntax) policies.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, NONE

priority Priority of the policy to be unbound. Minimum value: 1 Maximum value: 2147483647

bind feo global

Bind a front end optimization policy globally.

Synopsis

bind feo global <policyName> <priority>

Arguments

policyName Name of the front end optimization policy.

priority The priority assigned to the policy binding. Minimum value: 1 Maximum value: 2147483647

type Bind point, specifying where to bind the policy. This is relevant for advanced (default-syntax) policies only.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, NONE Default value: REQ_DEFAULT

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE. oIf gotoPriorityExpression is not present or if it is equal to END then the policy bank evaluation ends here oElse if the gotoPriorityExpression is equal to NEXT then the next policy in the priority order is evaluated. oElse gotoPriorityExpression is evaluated. The result of gotoPriorityExpression (which has to be a number) is processed as follows: -An UNDEF event is triggered if .gotoPriorityExpression cannot be evaluated .gotoPriorityExpression evaluates to number which is smaller than the maximum priority in the policy bank but is not same as any policy's priority .gotoPriorityExpression evaluates to a priority that is smaller than the current policy's priority -If the gotoPriorityExpression evaluates to the priority of the current policy then the next policy in the priority order is evaluated. -If the gotoPriorityExpression evaluates to the priority of a policy further ahead in the list then that policy will be evaluated next.

show feo global

Display the globally bound front end optimization policies.

Synopsis

show feo global

Arguments

type Bindpoint to which the policy is bound.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, NONE

Output

stateflag policyName The name of the globally bound front end optimization policy.

priority The priority assigned to the policy binding.

numpol The number of policies bound to the bindpoint.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

globalBindType devno count

feo-parameter

The following operations can be performed on "feo-parameter":

show| unset| set|

show feo parameter

Display front end optimization parameters

Synopsis

show feo parameter

Arguments

Output

JpegQualityPercent The percentage value of a JPEG image quality to be reduced. Range: 0 - 100

cssInlineThresSize Threshold value of the file size (in bytes) for converting external CSS files to inline CSS files.

jsInlineThresSize Threshold value of the file size (in bytes), for converting external JavaScript files to inline JavaScript files.

imgInlineThresSize Maximum file size of an image (in bytes), for coverting linked images to inline images.

builtin Specify the builtin flags for - set feo param.

feature The feature to be checked while applying this config

Example

show feo param

unset feo parameter

Use this command to remove feo parameter settings.Refer to the set feo parameter command for meanings of the arguments.

Synopsis

unset feo parameter

set feo parameter

Configure front end optimization parameters.

Synopsis

set feo parameter

Arguments

JpegQualityPercent The percentage value of a JPEG image quality to be reduced. Range: 0 - 100 Default value: 75 Minimum value: 0 Maximum value: 100

cssInlineThresSize Threshold value of the file size (in bytes) for converting external CSS files to inline CSS files. Default value: 1024 Minimum value: 1 Maximum value: 2048

jsInlineThresSize Threshold value of the file size (in bytes), for converting external JavaScript files to inline JavaScript files. Default value: 1024 Minimum value: 1 Maximum value: 2048

imgInlineThresSize Maximum file size of an image (in bytes), for coverting linked images to inline images. Default value: 1024 Minimum value: 1 Maximum value: 2048

Example

set feo param -JpegQualityPercent 80 -cssInlineThresSize 1024 -jsInlineThresSize 1024 -imgInlineThresSize 1024

feo-policy

The following operations can be performed on "feo-policy":

rm| set| unset| add| show|

rm feo policy

Remove a front end optimization policy.

Synopsis

rm feo policy <name>

Arguments

name The front end optimization policy to be removed.

set feo policy

Modify a front end optimization policy.

Synopsis

set feo policy <name>

Arguments

name The front end optimization policy to be modified.

rule The new rule to be associated with the front end optimization policy.

action The optimization to be associated with the front end optimization policy.

unset feo policy

Use this command to remove feo policy settings.Refer to the set feo policy command for meanings of the arguments.

Synopsis

unset feo policy <name>

add feo policy

Create a front end optimization policy.

Synopsis

add feo policy <name> <rule> <action>

Arguments

name The name of the front end optimization policy.

rule The rule associated with the front end optimization policy.

action The front end optimization action that has to be performed when the rule matches.

show feo policy

Display the configured front end optimization policies.

Synopsis

show feo policy

Arguments

name The name of the front end optimization policy.

Output

stateflag rule The rule associated with the front end optimization policy.

action The front end optimization action that has to be performed when the rule matches.

builtin Flag to determine if the front end optimization policy is built-in or not

feature The feature to be checked while applying this config

hits Total number of hits.

undefHits Total number of undefined policy hits.

activePolicy Indicates whether a policy is bound or not.

boundTo Location where the policy is bound to.

priority Priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

type devno count

feo-stats

The following operations can be performed on "feo-stats":

show feo stats

show feo stats is an alias for stat feo Displays Front end optimization statistics.

Synopsis

show feo stats - alias for 'stat feo'

feo

The following operations can be performed on "feo":

stat feo

Shows front end optimization performance statistics.

Synopsis

stat feo

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Optimized cache objects (VcDn) Total number of optimized cache objects ready to be served.

Original cache objects (OcDn) Total number of original cache objects ready to be served.

Domain Sharded (DmShd) Total no of images whose domain has been set from shards.

Images lazy loaded (ImLzLd) Total number of images modified for lazy loading.

URI Replaced (UrRep) Total number of URI replaced.

Inlined Imgs in CSS (InCsIm) Total number of images inlined in CSS.

Inlined JS (InJs) Total number of inlined JS files.

Inlined CSS (InCs) Total number of inlined CSS files.

Inlined images (InIm) Total number of inlined images in HTML.

Data Savings in KB (DatSav) Total data savings in bytes.

HTML comments removed (HtmCmtR) The total number of HTML comments removed.

Cache extended (CacExt) The total number of objects cache extended.

CSS combined (CssComb) The total number of CSS combined.

Import to Links (ImpToLink) The total number of CSS imports converted to links

JS moved to end (JsMoved) The total number of JS moved to end.

CSS moved to head (CssMoved) The total number of CSS moved to head.

JS Minifed (JsMin) The total number of JS files minified.

CSS Minifed (CssMin) The total number of CSS files minified.

Images to Jpegxr (ImgToJxr) The total number of images converted to JPEGXR format.

Images to WebP (ImgToWebP) The total number of images converted to WEBP format.

JPEGs Optimized (JpegsOpt) The total number of JPEG format images optimized.

Gif to PNGs (GifToPng) The total number of images converted from GIF to PNG format.

Images Resized (ImgResz) The total number of images resized to dimensions in the ▢

gslb

Gslb

The entities on which you can perform NetScaler CLI operations:

- gslb-config
- gslb-domain
- gslb-ldnsentries
- gslb-ldnsentry
- gslb-parameter
- gslb-runningConfig
- gslb-service
- gslb-serviceGroup
- gslb-serviceGroupMember
- gslb-site
- gslb-syncStatus
- gslb-vserver

gslb-config

The following operations can be performed on "gslb-config":

sync gslb config

Synchronizes the GSLB running configuration on all Citrix ADCs participating in the GSLB setup. The appliance on which this command is run is considered the master node. All GSLB sites configured on the master node and not having a parent site are synchronized with the master node.

Synopsis

sync gslb config

Arguments

preview Do not synchronize the GSLB sites, but display the commands that would be applied on the slave node upon synchronization. Mutually exclusive with the Save Configuration option.

debug Generate verbose output when synchronizing the GSLB sites. The Debug option generates more verbose output than the sync gslb config command in which the option is not used, and is useful for analyzing synchronization issues.

forceSync Force synchronization of the specified site even if a dependent configuration on the remote site is preventing synchronization or if one or more GSLB entities on the remote site have the same name but are of a different type. You can specify either the name of the remote site that you want to synchronize with the local site, or you can specify All Sites in the configuration utility (the string all-sites in the CLI). If you specify All Sites, all the sites in the GSLB setup are synchronized with the site on the master node. Note: If you select the Force Sync option, the synchronization starts without displaying the commands that are going to be executed.

nowarn Suppress the warning and the confirmation prompt that are displayed before site synchronization begins. This option can be used in automation scripts that must not be interrupted by a prompt.

saveconfig Save the configuration on all the nodes participating in the synchronization process, automatically. The master saves its configuration immediately before synchronization begins. Slave nodes save their configurations after the process of synchronization is complete. A slave node saves its configuration only if the configuration difference was successfully applied to it. Mutually exclusive with the Preview option.

command Run the specified command on the master node and then on all the slave nodes. You cannot use this option with the force sync and preview options.

Example

sync gslb config

gslb-domain

The following operations can be performed on "gslb-domain":

stat| show|

stat gslb domain

Displays the statistics associated with a global server load balancing (GSLB) domain.

Synopsis

stat gslb domain [<name>]

Arguments

name Name of the GSLB domain for which to display statistics. If you do not specify a name, statistics are shown for all configured GSLB domains.

dnsRecordType detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

domainHits (Hits) Total number of DNS queries received.

Dns Record Type (Rec_Type) Type of DNS record returned

Dns Record Type (Rec_Type) Type of DNS record returned

domainHits (Hits) Total number of DNS queries received.

Related Commands

- stat gslb serviceGroupMember

show gslb domain

Displays the bounded attributes of the domain.

Synopsis

show gslb domain

Arguments

name Name of the Domain

Output

serviceType The type GSLB service

state The state of the vserver

dnsRecordType The IP type for this GSLB vserver.

stateChangeTimeSec Time since last state change

lbMethod The load balancing method set for the virtual server

backupLBMethod Indicates the backup method in case the primary fails

persistenceType Indicates if persistence is set on the gslb vserver

persistenceId Persistence id of the gslb vserver

serviceName The service name.

vServerName siteName Name of the site to which the service belongs.

cip Indicates if Client IP option is enabled

sitePersistence Indicates the type of cookie persistence set

sitePrefix The site prefix string.

gslbthreshold The threshold value of the service

httpRequest HTTP request to the backend server

ipTunnel The state of the monitor for tunneled devices.

customHeaders The string that is sent to the service. Applicable to HTTP ,HTTP-ECV and RTSP monitor types.

respCode The response codes.

monitorName Monitor name

netmask Netmask

v6netmasklen Number of bits to consider, in an IPv6 source IP address, for creating the hash that is required by the SOURCEIPHASH load balancing method.

EDR Send clients an empty DNS response when the GSLB virtual server is DOWN.

MIR dynamicWeight Dynamic weight method of the vserver

persistMask The optional IPv4 network mask applied to IPv4 addresses to establish source IP address based persistence.

v6persistmasklen Number of bits to consider in an IPv6 source IP address when creating source IP address based persistence sessions.

IPAddress The Ip address of the service

port Port Number

weight weight assigned

dynamicConfWt dynamic weight

cumulativeWeight cumlative weight

svrEffGslbState GSLB server state

cnameEntry The cname of the gslb service

monState Monitor state

monitorTotalProbes Total monitor probes

monitorTotalFailedProbes Total probes failed

monitorCurrentFailedProbes Total number of current failed probes

monStatCode The code indicating the monitor response.

monStatParam1 First parameter for use with message code.

monStatParam2 Second parameter for use with message code.

monStatParam3 Third parameter for use with message code.

responseTime Response time of this monitor.

lastresponse The string form of monstatcode.

stateflag stateflag

serviceGroupName The GSLB service group name bound to the selected GSLB virtual server.

grpcHealthCheck The gRPC health check service status.

grpcStatusCode The gRPC status codes.

grpcServiceName The gRPC service name.

order Order number assigned to the service when it is bound to the gslb vserver.

devno count

gslb-ldnsentries

The following operations can be performed on "gslb-ldnsentries":

clear| show|

clear gslb ldnsentries

Clears all the local DNS (LDNS) entries created on the Citrix ADC. LDNS entries store network metrics for RTT learned from the packets exchanged with LDNS servers.

Synopsis

clear gslb ldnsentries

show gslb ldnsentries

Displays the local DNS (LDNS) entries created on the Citrix ADC. LDNS entries store network metrics for RTT learned from the packets exchanged with LDNS servers.

Synopsis

show gslb ldnsentries

Arguments

Output

siteName The GSLB site name

numsites Specifies the number of gslb sites

IPAddress IP address of the LDNS server

TTL TTL value of the LDNS entry

name Monitor that is currently being used to monitor the LDNS ip..

rtt RTT value of the LDNS entry for all gslb sites

devno count stateflag

Example

show gslb ldnsentries

gslb-ldnsentry

The following operations can be performed on "gslb-ldnsentry":

rm gslb ldnsentry

Removes the LDNS entry for the specified LDNS IP address.

Synopsis

rm gslb ldnsentry <IPAddress>

Arguments

IPAddress IP address of the LDNS server.

Example

rm gslb ldnsentry 10.102.27.226

gslb-parameter

The following operations can be performed on "gslb-parameter":

set| unset| show|

set gslb parameter

Sets various global GSLB parameters.

Synopsis

set gslb parameter

Arguments

ldnsEntryTimeout Time, in seconds, after which an inactive LDNS entry is removed. Default value: 180 Minimum value: 30 Maximum value: 65534

RTTTolerance Tolerance, in milliseconds, for newly learned round-trip time (RTT) values. If the difference between the old RTT value and the newly computed RTT value is less than or equal to the specified tolerance value, the LDNS entry in the network metric table is not updated with the new RTT value. Prevents the exchange of metrics when variations in RTT values are negligible. Default value: 5 Minimum value: 1 Maximum value: 100

ldnsMask The IPv4 network mask with which to create LDNS entries. Default value: 0xFFFFFFFF

v6ldnsmasklen Mask for creating LDNS entries for IPv6 source addresses. The mask is defined as the number of leading bits to consider, in the source IP address, when creating an LDNS entry. Default value: 128 Minimum value: 1 Maximum value: 128

ldnsProbeOrder Order in which monitors should be initiated to calculate RTT.

Possible values: PING, DNS, TCP Default value: ARRAY(0x2bac94c4)

dropLdnsReq Drop LDNS requests if round-trip time (RTT) information is not available.

Possible values: ENABLED, DISABLED Default value: DISABLED

GSLBSvcStateDelayTime Amount of delay in updating the state of GSLB service to DOWN when MEP goes down. This parameter is applicable only if monitors are not bound to GSLB services Default value: 0 Maximum value: 3600

SvcStateLearningTime Time (in seconds) within which local or child site services remain in learning phase. GSLB site will enter the learning phase after reboot, HA failover, Cluster GSLB owner node changes or MEP being enabled on local node. Backup parent (if configured) will selectively move the adopted children's GSLB services to learning phase when primary parent goes down. While a service is in learning period, remote site will not honour the state and stats got through MEP for that service. State can be learnt from health monitor if bound explicitly. Default value: 0 Maximum value: 3600

AutomaticConfigSync GSLB configuration will be synced automatically to remote gslb sites if enabled.

Possible values: ENABLED, DISABLED Default value: DISABLED

MEPKeepAliveTimeout Time duartion (in seconds) during which if no new packets received by Local gslb site from Remote gslb site then mark the MEP connection DOWN Default value: 10 Minimum value: 1

GSLBSyncInterval Time duartion (in seconds) for which the gslb sync process will wait before checking for config changes. Default value: 10 Minimum value: 1

GSLBSyncMode Mode in which configuration will be synced from master site to remote sites.

Possible values: IncrementalSync, FullSync Default value: IncrementalSync

GSLBSyncLocFiles If disabled, Location files will not be synced to the remote sites as part of automatic sync.

Possible values: ENABLED, DISABLED Default value: ENABLED

GslbConfigSyncMonitor If enabled, remote gslb site's rsync port will be monitored and site is considered for configuration sync only when the monitor is successful.

Possible values: ENABLED, DISABLED Default value: DISABLED

GSLBSyncSaveConfigCommand If enabled, 'save ns config' command will be treated as other GSLB commands and synced to GSLB nodes when auto gslb sync option is enabled.

Possible values: ENABLED, DISABLED Default value: DISABLED

undefAction Action to perform when policy evaluation creates an UNDEF condition. Available settings function as follows:

- NOLBACTION - Does not consider LB action in making LB decision.
- RESET - Reset the request and notify the user, so that the user can resend the request.
- DROP - Drop the request without sending a response to the user. Default value: "NOLBACTION"

Example

set gslb parameter -ldnsMask 255.255.0.0

unset gslb parameter

Use this command to remove gslb parameter settings.Refer to the set gslb parameter command for meanings of the arguments.

Synopsis

unset gslb parameter

show gslb parameter

Displays the global GSLB parameters.

Synopsis

show gslb parameter

Arguments

Output

flags State of the GSLB parameter.

ldnsEntryTimeout Time, in seconds, after which an inactive LDNS entry is removed.

RTTTolerance Tolerance, in milliseconds, for newly learned round-trip time (RTT) values. If the difference between the old RTT value and the newly computed RTT value is less than or equal to the specified tolerance value, the LDNS entry in the network metric table is not updated with the new RTT value. Prevents the exchange of metrics when variations in RTT values are negligible.

ldnsMask The IPv4 network mask with which to create LDNS entries.

v6ldnsmasklen Mask for creating LDNS entries for IPv6 source addresses. The mask is defined as the number of leading bits to consider, in the source IP address, when creating an LDNS entry.

ldnsProbeOrder The order in which monitors should be initiated to calculate RTT

dropLdnsReq Drop LDNS requests if round-trip time (RTT) information is not available.

GSLBSvcStateDelayTime Amount of delay in updating the state of GSLB service to DOWN when MEP goes down. This parameter is applicable only if monitors are not bound to GSLB services

SvcStateLearningTime Time (in seconds) within which local or child site services remain in learning phase. GSLB site will enter the learning phase after reboot, HA failover, Cluster GSLB owner node changes or MEP being enabled on local node. Backup parent (if configured) will selectively move the adopted children's GSLB services to learning phase when primary parent goes down. While a service is in learning period, remote site will not honour the state and stats got through MEP for that service. State can be learnt from health monitor if bound explicitly.

AutomaticConfigSync GSLB configuration will be synced automatically to remote gslb sites if enabled.

builtin feature The feature to be checked while applying this config

MEPKeepAliveTimeout Time duartion (in seconds) during which if no new packets received by Local gslb site from Remote gslb site then mark the MEP connection DOWN

GSLBSyncInterval Time duartion (in seconds) for which the gslb sync process will wait before checking for config changes.

GSLBSyncMode Mode in which configuration will be synced from master site to remote sites.

incarnation This is a counter to maintain the gslb sync incarnation number.

GSLBSyncLocFiles If disabled, Location files will not be synced to the remote sites as part of automatic sync.

GslbConfigSyncMonitor If enabled, remote gslb site's rsync port will be monitored and site is considered for configuration sync only when the monitor is successful.

GSLBSyncSaveConfigCommand If enabled, 'save ns config' command will be treated as other GSLB commands and synced to GSLB nodes when auto gslb sync option is enabled.

undefAction Action to perform when policy evaluation creates an UNDEF condition. Available settings function as follows:

- NOLBACTION - Does not consider LB action in making LB decision.
- RESET - Reset the request and notify the user, so that the user can resend the request.
- DROP - Drop the request without sending a response to the user.

overridePersistencyforOrder This option is used to override persistency when order is configured for services or servicegroups.

Example

show gslb parameter

gslb-runningConfig

The following operations can be performed on "gslb-runningConfig":

show gslb runningConfig

Displays the complete GSLB configuration running on the Citrix ADC. In addition to the saved configuration, the running configuration includes GSLB settings that have not yet been saved to the Citrix ADC configuration file (ns.conf).

Synopsis

show gslb runningConfig

Arguments

Output

response gslb sync status as text blob

Related Commands

- show ns.conf

gslb-service

The following operations can be performed on "gslb-service":

stat| bind| set| rename| unbind| show| add| unset| rm|

stat gslb service

Displays the statistical data collected for a global server load balancing (GSLB) service.

Synopsis

stat gslb service

Arguments

serviceName Name of the GSLB service.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Current Client Est connections (ClntEstConn) Number of client connections in ESTABLISHED state.

IP address (IP) The IP address on which the service is running.

Port (port) The port on which the service is running.

Service type (Type) The service type of this service.Possible values are ADNS, DNS, MYSQL, RTSP, SSL_DIAMETER, ADNS_TCP, DNS_TCP, NNTP, SIP_UDP, SSL_TCP, ANY, FTP, RADIUS, SNMP, TCP, DHCPRA, HTTP, RDP, SSL, TFTP, DIAMETER, MSSQL, RPCSVR, SSL_BRIDGE, UDP

State Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)

Request bytes (Reqb) Total number of request bytes received on this service or virtual server.

Response bytes (Rspb) Number of response bytes received by this service or virtual server.

Current load on the service (Load) Load on the service that is calculated from the bound load based monitor.

Requests (Req) Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Responses (Rsp) Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Current client connections (ClntConn) Number of current client connections.

Current server connections (SvrConn) Number of current connections to the actual servers behind the virtual server.

Service hits (Hits) Number of times that the service has been provided.

Binding Order (Order) Order with which service is bound to vserver

Current Server Est connections (SvrEstConn) Number of server connections in ESTABLISHED state.

Related Commands

- stat gslb serviceGroupMember

bind gslb service

Binds a DNS view or a monitor to a global server load balancing (GSLB) service.

Synopsis

bind gslb service <serviceName> ((-viewName <string> <viewIP>) | (-monitorName <string>@))

Arguments

serviceName Name of the GSLB service.

viewName Name of the DNS view of the service. A DNS view is used in global server load balancing (GSLB) to return a predetermined IP address to a specific group of clients, which are identified by using a DNS policy.

viewIP IP address for the specified DNS view.

monitorName Name of the monitor to bind to the GSLB service.

monState Initial state of the GSLB monitor.

Possible values: ENABLED, DISABLED Default value: ENABLED

weight Weight to assign to the monitor-service binding. A larger number specifies a greater weight. Contributes to the monitoring threshold, which determines the state of the service. Default value: 1 Minimum value: 1 Maximum value: 100

Example

bind gslb service -viewName privateview 1.2.3.4

set gslb service

Modifies the specified parameters of a global server load balancing (GSLB) service.

Synopsis

set gslb service <serviceName> [-cip (ENABLED | DISABLED)] [-naptrReplacement <string>]

Arguments

serviceName Name of the GSLB service.

IPAddress The new IP address of the service.

publicIP The public IP address that a NAT device translates to the GSLB service's private IP address. Optional.

publicPort The public port associated with the GSLB service's public IP address. The port is mapped to the service's private port number. Applicable to the local GSLB service. Optional. Minimum value: 1

cip In the request that is forwarded to the GSLB service, insert a header that stores the client's IP address. Client IP header insertion is used in connection-proxy based site persistence.

Possible values: ENABLED, DISABLED Default value: DISABLED

cipHeader Name for the HTTP header that stores the client's IP address. Used with the Client IP option. If client IP header insertion is enabled on the service and a name is not specified for the header, the Citrix ADC uses the name specified by the cipHeader parameter in the set ns param command or, in the GUI, the Client IP Header parameter in the Configure HTTP Parameters dialog box.

sitePersistence Use cookie-based site persistence. Applicable only to HTTP and SSL GSLB services.

Possible values: ConnectionProxy, HTTPRedirect, NONE

sitePrefix The site's prefix string. When the service is bound to a GSLB virtual server, a GSLB site domain is generated internally for each bound service-domain pair by concatenating the site prefix of the service and the name of the domain. If the special string NONE is specified, the site-prefix string is unset. When implementing HTTP redirect site persistence, the Citrix ADC redirects GSLB requests to GSLB services by using their site domains.

maxClient The maximum number of open connections that the service can support at any given time. A GSLB service whose connection count reaches the maximum is not considered when a GSLB decision is made, until the connection count drops below the maximum. Minimum value: 0 Maximum value: 4294967294

healthMonitor Monitor the health of the GSLB service.

Possible values: YES, NO Default value: YES

maxBandwidth Maximum bandwidth. Minimum value: 0

downStateFlush Flush all active transactions associated with the GSLB service when its state transitions from UP to DOWN. Do not enable this option for services that must complete their transactions. Applicable if connection proxy based site persistence is used.

Possible values: ENABLED, DISABLED Default value: ENABLED

maxAAAUsers Maximum number of SSL VPN users that can be logged on concurrently to the VPN virtual server that is represented by this GSLB service. A GSLB service whose user count reaches the maximum is not considered when a GSLB decision is made, until the count drops below the maximum. Minimum value: 0 Maximum value: 65535

viewName Name of the DNS view of the service. A DNS view is used in global server load balancing (GSLB) to return a predetermined IP address to a specific group of clients, which are identified by using a DNS policy.

viewIP IP address to be used for the given view

monThreshold Monitoring threshold value for the GSLB service. If the sum of the weights of the monitors that are bound to this GSLB service and are in the UP state is not equal to or greater than this threshold value, the service is marked as DOWN. Minimum value: 0 Maximum value: 65535

weight Weight to assign to the monitor-service binding. A larger number specifies a greater weight. Contributes to the monitoring threshold, which determines the state of the service. Minimum value: 1 Maximum value: 100

monitorName Name of the monitor to bind to the service.

hashId Unique hash identifier for the GSLB service, used by hash based load balancing methods. Minimum value: 1

comment Any comments that you might want to associate with the GSLB service.

appflowLog Enable logging appflow flow information

Possible values: ENABLED, DISABLED Default value: ENABLED

naptrOrder An integer specifying the order in which the NAPTR records MUST be processed in order to accurately represent the ordered list of Rules. The ordering is from lowest to highest Default value: 1 Minimum value: 1 Maximum value: 65535

naptrPreference An integer specifying the preference of this NAPTR among NAPTR records having same order. lower the number, higher the preference. Default value: 1 Minimum value: 1 Maximum value: 65535

naptrServices Service Parameters applicable to this delegation path.

naptrReplacement The replacement domain name for this NAPTR.

naptrDomainTTL Modify the TTL of the internally created naptr domain Default value: 3600 Minimum value: 1

Example

set gslb service sj_svc -sitePersistence ConnectionProxy

rename gslb service

Renames a global server load balancing (GSLB) service.

Synopsis

rename gslb service <serviceName>@ <newName>@

Arguments

serviceName Existing name of the GSLB service.

newName New name for the GSLB service.

Example

rename gslb service gsl_svc gslb_svc_new

unbind gslb service

Unbinds a DNS view or a monitor from a global server load balancing (GSLB) service.

Synopsis

unbind gslb service <serviceName> (-viewName <string> | -monitorName <string>@)

Arguments

serviceName Name of the GSLB service.

viewName Name of the DNS view of the service. A DNS view specifies the IP address that must be returned to clients accessing the service from a specific location.

monitorName Name of the monitor to unbind.

Example

unbind gslb service -viewName privateview

show gslb service

Displays the parameters of all the global server load balancing (GSLB) services configured on the appliance, or the parameters of just the specified service, and statistics related to the service. To display the parameters of all the GSLB services, do not specify a service name.

Synopsis

show gslb service show gslb service stats - alias for 'stat gslb service'

Arguments

serviceName Name of the GSLB service.

Output

gslb IPAddress IP address of the service

IP IP address of the service

serverName Name of the server hosting the GSLB service.

serviceType Service type.

port Port number of the service.

publicIP Public ip of the service

publicPort Public port of the service

maxClient Maximum number of clients.

maxAAAUsers Maximum number of SSL VPN users that can be logged on concurrently to the VPN virtual server that is represented by this GSLB service. A GSLB service whose user count reaches the maximum is not considered when a GSLB decision is made, until the count drops below the maximum.

siteName Name of the site to which the service belongs.

svrState Server state.

svrEffGslbState Effective state of the gslb svc

gslbthreshold Indicates if gslb svc has reached threshold

gslbsvcStats Indicates if gslb svc has stats of the primary or the whole chain

state Enable or disable the service.

monitorName Monitor name.

monState State of the monitor bound to gslb service.

cip Indicates if Client IP option is enabled

cipHeader The client IP header used in the HTTP request.

sitePersistence Indicates the type of cookie persistence set

sitePrefix The site prefix string.

cltTimeout Client timeout in seconds.

svrTimeout Server timeout in seconds.

totalfailedprobes The total number of failed probs.

preferredLocation Prefered location.

maxBandwidth Maximum bandwidth.

downStateFlush Flush all active transactions associated with the GSLB service when its state transitions from UP to DOWN. Do not enable this option for services that must complete their transactions. Applicable if connection proxy based site persistence is used.

cnameEntry Canonical name of the GSLB service. Used in CNAME-based GSLB.

viewName Name of the DNS view of the service. A DNS view is used in global server load balancing (GSLB) to return a predetermined IP address to a specific group of clients, which are identified by using a DNS policy.

viewIP IP address to be used for the given view

weight The Weight of monitor

monThreshold Monitoring threshold value for the GSLB service. If the sum of the weights of the monitors that are bound to this GSLB service and are in the UP state is not equal to or greater than this threshold value, the service is marked as DOWN.

failedprobes Number of the current failed monitoring probes.

monStatCode The code indicating the monitor response.

monStatParam1 First parameter for use with message code.

monStatParam2 Second parameter for use with message code.

monStatParam3 Third parameter for use with message code.

responseTime Response time of this monitor.

monState The running state of the monitor on this service.

hashId Unique hash identifier for the GSLB service, used by hash based load balancing methods.

comment Any comments that you might want to associate with the GSLB service.

stateflag stateflag

healthMonitor Monitor the health of the GSLB service.

appflowLog Enable logging appflow flow information

svccfgFlags Contains the information about config info like internal/configured service

monitorTotalProbes Total number of probes sent to monitor this service.

monitorTotalFailedProbes Total number of failed probes

monitorCurrentFailedProbes Total number of currently failed probes

stateChangeTimeSec Time when last state change happened. Seconds part.

ticksSinceLastStateChange Time in 10 millisecond ticks since the last state change.

threshold ClMonOwner Tells the mon owner of the gslb service.

ClMonView Tells the view id of the monitoring owner.

lastresponse Displays the gslb monitor status in string format.

naptrOrder An integer specifying the order in which the NAPTR records MUST be processed in order to accurately represent the ordered list of Rules. The ordering is from lowest to highest

naptrPreference An integer specifying the preference of this NAPTR among NAPTR records having same order. lower the number, higher the preference.

naptrServices Service Parameters applicable to this delegation path.

naptrReplacement The replacement domain name for this NAPTR.

naptrDomainTTL Modify the TTL of the internally created naptr domain

gslbsvcHealth This parameter displays effective health of a GSLB service.

glsbsvcHealthdescr Displays the warning message related to health a of GSLB service.

noDefaultBindings to determine if the configuration will have default ssl CIPHER and ECC curve bindings

devno count

Example

show gslb service sj_svc

add gslb service

Creates a global server load balancing (GSLB) service.

Synopsis

add gslb service <serviceName> (-cnameEntry <string> | <IP> | <serverName> | <serviceType> | <port> | -publicIP <ip_addr|ipv6_addr|*> | -publicPort <port> | -sitePersistence <sitePersistence> | -sitePrefix <string>) -siteName <string> [-cip (ENABLED | DISABLED)] [-naptrReplacement <string>]

Arguments

serviceName Name for the GSLB service. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the GSLB service is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my gslbsvc" or 'my gslbsvc').

cnameEntry Canonical name of the GSLB service. Used in CNAME-based GSLB.

IP IP address for the GSLB service. Should represent a load balancing, content switching, or VPN virtual server on the Citrix ADC, or the IP address of another load balancing device.

serverName Name of the server hosting the GSLB service.

serviceType Type of service to create.

Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, ANY, SIP_UDP, SIP_TCP, SIP_SSL, RADIUS, RDP, RTSP, MYSQL, MSSQL, ORACLE Default value: NSSVC_SERVICE_UNKNOWN

port Port on which the load balancing entity represented by this GSLB service listens. Minimum value: 1

publicIP The public IP address that a NAT device translates to the GSLB service's private IP address. Optional.

publicPort The public port associated with the GSLB service's public IP address. The port is mapped to the service's private port number. Applicable to the local GSLB service. Optional.

maxClient The maximum number of open connections that the service can support at any given time. A GSLB service whose connection count reaches the maximum is not considered when a GSLB decision is made, until the connection count drops below the maximum. Minimum value: 0 Maximum value: 4294967294

healthMonitor Monitor the health of the GSLB service.

Possible values: YES, NO Default value: YES

siteName Name of the GSLB site to which the service belongs.

state Enable or disable the service.

Possible values: ENABLED, DISABLED Default value: ENABLED

cip In the request that is forwarded to the GSLB service, insert a header that stores the client's IP address. Client IP header insertion is used in connection-proxy based site persistence.

Possible values: ENABLED, DISABLED Default value: DISABLED

cipHeader Name for the HTTP header that stores the client's IP address. Used with the Client IP option. If client IP header insertion is enabled on the service and a name is not specified for the header, the Citrix ADC uses the name specified by the cipHeader parameter in the set ns param command or, in the GUI, the Client IP Header parameter in the Configure HTTP Parameters dialog box.

sitePersistence Use cookie-based site persistence. Applicable only to HTTP and SSL GSLB services.

Possible values: ConnectionProxy, HTTPRedirect, NONE

cookieTimeout Timeout value, in minutes, for the cookie, when cookie based site persistence is enabled. Maximum value: 1440

sitePrefix The site's prefix string. When the service is bound to a GSLB virtual server, a GSLB site domain is generated internally for each bound service-domain pair by concatenating the site prefix of the service and the name of the domain. If the special string NONE is specified, the site-prefix string is unset. When implementing HTTP redirect site persistence, the Citrix ADC redirects GSLB requests to GSLB services by using their site domains.

cltTimeout Idle time, in seconds, after which a client connection is terminated. Applicable if connection proxy based site persistence is used. Maximum value: 31536000

svrTimeout Idle time, in seconds, after which a server connection is terminated. Applicable if connection proxy based site persistence is used. Maximum value: 31536000

maxBandwidth Integer specifying the maximum bandwidth allowed for the service. A GSLB service whose bandwidth reaches the maximum is not considered when a GSLB decision is made, until its bandwidth consumption drops below the maximum. Minimum value: 0

downStateFlush Flush all active transactions associated with the GSLB service when its state transitions from UP to DOWN. Do not enable this option for services that must complete their transactions. Applicable if connection proxy based site persistence is used.

Possible values: ENABLED, DISABLED

maxAAAUsers Maximum number of SSL VPN users that can be logged on concurrently to the VPN virtual server that is represented by this GSLB service. A GSLB service whose user count reaches the maximum is not considered when a GSLB decision is made, until the count drops below the maximum. Minimum value: 0 Maximum value: 65535

monThreshold Monitoring threshold value for the GSLB service. If the sum of the weights of the monitors that are bound to this GSLB service and are in the UP state is not equal to or greater than this threshold value, the service is marked as DOWN. Minimum value: 0 Maximum value: 65535

hashId Unique hash identifier for the GSLB service, used by hash based load balancing methods. Minimum value: 1

comment Any comments that you might want to associate with the GSLB service.

appflowLog Enable logging appflow flow information

Possible values: ENABLED, DISABLED Default value: ENABLED

naptrReplacement The replacement domain name for this NAPTR.

naptrOrder An integer specifying the order in which the NAPTR records MUST be processed in order to accurately represent the ordered list of Rules. The ordering is from lowest to highest Default value: 1 Minimum value: 1 Maximum value: 65535

naptrServices Service Parameters applicable to this delegation path.

naptrDomainTTL Modify the TTL of the internally created naptr domain Default value: 3600 Minimum value: 1

naptrPreference An integer specifying the preference of this NAPTR among NAPTR records having same order. lower the number, higher the preference. Default value: 1 Minimum value: 1 Maximum value: 65535

Example

add gslb service sj_svc 203.12.123.12 http 80 -site san_jos

unset gslb service

Use this command to remove gslb service settings.Refer to the set gslb service command for meanings of the arguments.

Synopsis

unset gslb service <serviceName>

rm gslb service

Removes a global server load balancing (GSLB) service configured on the appliance.

Synopsis

rm gslb service <serviceName>

Arguments

serviceName Name of the GSLB service.

Example

rm gslb service sj_svc

gslb-serviceGroup

The following operations can be performed on "gslb-serviceGroup":

add| rm| enable| show| set| rename| stat| disable| unset| unbind| bind|

add gslb serviceGroup

Creates a GSLB service group. You can group similar services into a GSLB service group and use them as a single entity.

Synopsis

add gslb serviceGroup <serviceGroupName>@ <serviceType> [-cip (ENABLED | DISABLED)] [-autoScale (DISABLED | DNS)] -siteName <string>

Arguments

serviceGroupName Name of the GSLB service group. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the name is created.

serviceType Protocol used to exchange data with the GSLB service.

Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, ANY, SIP_UDP, SIP_TCP, SIP_SSL, RADIUS, RDP, RTSP, MYSQL, MSSQL, ORACLE

maxClient Maximum number of simultaneous open connections for the GSLB service group. Minimum value: 0 Maximum value: 4294967294

cip Insert the Client IP header in requests forwarded to the GSLB service.

Possible values: ENABLED, DISABLED

cipHeader Name of the HTTP header whose value must be set to the IP address of the client. Used with the Client IP parameter. If client IP insertion is enabled, and the client IP header is not specified, the value of Client IP Header parameter or the value set by the set ns config command is used as client's IP header name.

healthMonitor Monitor the health of this GSLB service.Available settings function are as follows: YES - Send probes to check the health of the GSLB service. NO - Do not send probes to check the health of the GSLB service. With the NO option, the appliance shows the service as UP at all times.

Possible values: YES, NO Default value: YES

cltTimeout Time, in seconds, after which to terminate an idle client connection. Maximum value: 31536000

svrTimeout Time, in seconds, after which to terminate an idle server connection. Maximum value: 31536000

maxBandwidth Maximum bandwidth, in Kbps, allocated for all the services in the GSLB service group. Minimum value: 0 Maximum value: 4294967287

monThreshold Minimum sum of weights of the monitors that are bound to this GSLB service. Used to determine whether to mark a GSLB service as UP or DOWN. Minimum value: 0 Maximum value: 65535

state Initial state of the GSLB service group.

Possible values: ENABLED, DISABLED Default value: ENABLED

downStateFlush Flush all active transactions associated with all the services in the GSLB service group whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions.

Possible values: ENABLED, DISABLED Default value: ENABLED

comment Any information about the GSLB service group.

appflowLog Enable logging of AppFlow information for the specified GSLB service group.

Possible values: ENABLED, DISABLED Default value: ENABLED

autoScale Auto scale option for a GSLB servicegroup

Possible values: DISABLED, DNS Default value: DISABLED

autoDelayedTrofs Indicates graceful movement of the service to TROFS. System will wait for monitor response time out before moving to TROFS

Possible values: YES, NO Default value: NO

siteName Name of the GSLB site to which the service group belongs.

sitePersistence Use cookie-based site persistence. Applicable only to HTTP and SSL non-autoscale enabled GSLB servicegroups.

Possible values: ConnectionProxy, HTTPRedirect, NONE

Example

add gslb servicegroup http_svc_group http -site san_jos

rm gslb serviceGroup

Removes a GSLB service group.

Synopsis

rm gslb serviceGroup <serviceGroupName>@

Arguments

serviceGroupName Name of the GSLB service group.

Example

rm gslb servicegroup http_svc_group

enable gslb serviceGroup

Enables a GSLB service group or a member of the GSLB service group.

Synopsis

enable gslb serviceGroup <serviceGroupName>@

Arguments

serviceGroupName Name of the gslb service group.

serverName Name of the server that hosts the gslb service.

port Port number of the service to be enabled.

Example

enable gslb servicegroup http_svc_group

Related Commands

- enable GSLB service

show gslb serviceGroup

Displays the specified GSLB service group's binding information.

Synopsis

show gslb serviceGroup

Arguments

serviceGroupName Name of the GSLB service group.

includeMembers Display the members of the listed GSLB service groups in addition to their settings. Can be specified when no service group name is provided in the command. In that case, the details displayed for each service group are identical to the details displayed when a service group name is provided, except that bound monitors are not displayed.

Output

numOfconnections This will tell the number of client side connections are still open.

serviceType Protocol used to exchange data with the GSLB service.

port The port number of the GSLB service to be enabled.

serviceConfType The configuration type of the GSLB service group.

value SSL Status.

maxClient Maximum number of simultaneous open connections for the GSLB service group.

cip Insert the Client IP header in requests forwarded to the GSLB service.

cipHeader CIP Header.

monweight weight of the monitor that is bound to GSLB servicegroup.

cltTimeout Time, in seconds, after which to terminate an idle client connection.

svrTimeout Time, in seconds, after which to terminate an idle server connection.

maxBandwidth Maximum bandwidth, in Kbps, allocated for all the services in the GSLB service group.

state The state of the GSLB service group

svrState The state of the GSLB service

delay The remaining time in seconds for the service to be disabled

IP IP Address.

serverName The name of the server to be changed.

monitorName Monitor name.

monThreshold Minimum sum of weights of the monitors that are bound to this GSLB service. Used to determine whether to mark a GSLB service as UP or DOWN.

monState Monitor state.

weight When used along with monitor name, it specifies the weight of the monitor binding. When used along with servername & port pair, it specifies the weight of this GSLB service .

monState The running state of the monitor on this service.

monStatCode The code indicating the monitor response.

monStatParam1 First parameter for use with message code.

monStatParam2 Second parameter for use with message code.

monStatParam3 Third parameter for use with message code.

monitorTotalProbes Total number of probes sent to monitor this service.

monitorTotalFailedProbes Total number of failed probes

monitorCurrentFailedProbes Total number of currently failed probes

downStateFlush Flush all active transactions associated with all services in the GSLB service group whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions.

lastresponse The string form of monstatcode.

stateChangeTimeSec Time when last state change occurred. Seconds part.

stateChangeTimemSec Time when last state change occurred. Milliseconds part.

ticksSinceLastStateChange Time in 10 millisecond ticks since the last state change.

StateUpdateReason Checks state update reason on the secondary node.

ClMonOwner Tells the mon owner of the service.

ClMonView Tells the view id of the monitoring owner.

groupCount Servicegroup Count

comment Any information about the GSLB service group.

hashId The hash identifier for the service. This must be unique for each service. This parameter is used by hash based load balancing methods.

graceFul Indicates graceful shutdown of the GSLB service. System will wait for all outstanding connections to this service to be closed before disabling the service.

healthMonitor Monitor the health of this GSLB service.Available settings function are as follows: YES - Send probes to check the health of the GSLB service. NO - Do not send probes to check the health of the GSLB service. With the NO option, the appliance shows the service as UP at all times.

appflowLog Enable logging of AppFlow information for the specified GSLB service group.

autoScale Auto scale option for a GSLB servicegroup

autoDelayedTrofs Indicates graceful movement of the service to TROFS. System will wait for monitor response time out before moving to TROFS

state Monitor state.

weight weight of the monitor that is bound to GSLB servicegroup.

serviceIPstr This field has been intorduced to show the dbs services ip

serviceGroupEntName2 passive Indicates if load monitor is passive. A passive load monitor does not remove service from LB decision when threshold is breached.

serviceGroupeffectivestate Indicates the effective GSLB servicegroup state based on the state of the bound service items.If all services are UP the effective state is UP, if all are DOWN its DOWN,if all are OFS its OFS.If atleast one serviceis UP and rest are either DOWN or OFS, the effective state is PARTIAL-UP.If atleast one bound service is DOWN and rest are OFS the effective state is PARTIAL DOWN.

siteName Name of the site to which the GSLB service group belongs.

gslb publicIP The public IP address that a NAT device translates to the GSLB service's private IP address. Optional.

publicPort The public port associated with the GSLB service's public IP address. The port is mapped to the service's private port number. Applicable to the local GSLB service. Optional.

svrEffGslbState Effective state of the gslb svc

gslbthreshold Indicates if gslb svc has reached threshold

threshold preferredLocation Prefered location.

sitePersistence Use cookie-based site persistence. Applicable only to HTTP and SSL non-autoscale enabled GSLB servicegroups.

sitePrefix The site's prefix string. When the GSLB service group is bound to a GSLB virtual server, a GSLB site domain is generated internally for each bound serviceitem-domain pair by concatenating the site prefix of the service item and the name of the domain. If the special string NONE is specified, the site-prefix string is unset. When implementing HTTP redirect site persistence, the Citrix ADC redirects GSLB requests to GSLB services by using their site domains.

noDefaultBindings to determine if the configuration is from stylebooks

order Order number to be assigned to the gslb servicegroup member

order Order number in string form assigned to the gslb servicegroup member

trofsDelay Delay before moving to TROFS

devno count stateflag

set gslb serviceGroup

Modifies the specified parameters of a GSLB service group.

Synopsis

set gslb serviceGroup <serviceGroupName>@ [(<serverName>@ <port>) | -maxClient <positive_integer> | -cip (ENABLED | DISABLED) | <cipHeader> | -cltTimeout <secs> | -svrTimeout <secs> | -maxBandwidth <positive_integer> | -monThreshold <positive_integer> | -downStateFlush (ENABLED | DISABLED) | -sitePersistence <sitePersistence>]

Arguments

serviceGroupName Name of the GSLB service group.

serverName Name of the server to which to bind the service group.

port Server port number.

weight Weight to assign to the servers in the service group. Specifies the capacity of the servers relative to the other servers in the load balancing configuration. The higher the weight, the higher the percentage of requests sent to the service. Minimum value: 1 Maximum value: 100

hashId The hash identifier for the service. This must be unique for each service. This parameter is used by hash based load balancing methods. Minimum value: 1

publicIP The public IP address that a NAT device translates to the GSLB service's private IP address. Optional.

publicPort The public port associated with the GSLB service's public IP address. The port is mapped to the service's private port number. Applicable to the local GSLB service. Optional. Minimum value: 1

sitePrefix The site's prefix string. When the GSLB service group is bound to a GSLB virtual server, a GSLB site domain is generated internally for each bound serviceitem-domain pair by concatenating the site prefix of the service item and the name of the domain. If the special string NONE is specified, the site-prefix string is unset. When implementing HTTP redirect site persistence, the Citrix ADC redirects GSLB requests to GSLB services by using their site domains.

order Order number to be assigned to the gslb servicegroup member Minimum value: 1 Maximum value: 8192

monitorName Name of the monitor bound to the GSLB service group. Used to assign a weight to the monitor.

weight weight of the monitor that is bound to GSLB servicegroup. Minimum value: 1

maxClient Maximum number of simultaneous open connections for the GSLB service group. Minimum value: 0 Maximum value: 4294967294

healthMonitor Monitor the health of this GSLB service.Available settings function are as follows: YES - Send probes to check the health of the GSLB service. NO - Do not send probes to check the health of the GSLB service. With the NO option, the appliance shows the service as UP at all times.

Possible values: YES, NO Default value: YES

cip Insert the Client IP header in requests forwarded to the GSLB service.

Possible values: ENABLED, DISABLED

cipHeader CIP Header.

cltTimeout Time, in seconds, after which to terminate an idle client connection. Maximum value: 31536000

svrTimeout Time, in seconds, after which to terminate an idle server connection. Maximum value: 31536000

maxBandwidth Maximum bandwidth, in Kbps, allocated for all the services in the GSLB service group. Minimum value: 0 Maximum value: 4294967287

monThreshold Minimum sum of weights of the monitors that are bound to this GSLB service. Used to determine whether to mark a GSLB service as UP or DOWN. Minimum value: 0 Maximum value: 65535

downStateFlush Flush all active transactions associated with all the services in the GSLB service group whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions.

Possible values: ENABLED, DISABLED Default value: ENABLED

comment Any information about the GSLB service group.

appflowLog Enable logging of AppFlow information for the specified GSLB service group.

Possible values: ENABLED, DISABLED Default value: ENABLED

sitePersistence Use cookie-based site persistence. Applicable only to HTTP and SSL non-autoscale enabled GSLB servicegroups.

Possible values: ConnectionProxy, HTTPRedirect, NONE

Example

set gslb servicegroup http_svc_group -maxClient 100

rename gslb serviceGroup

Renames a global server load balancing (GSLB) servicegroup. Please fire this command manually or by using real time sync on all the participating GSLB sites otherwise stats exchange between GSLB sites will not work.

Synopsis

rename gslb serviceGroup <serviceGroupName>@ <newName>@

Arguments

serviceGroupName Existing name of the GSLB service group.

newName New name for the GSLB service group.

Example

rename gslb servicegroup gslb_svc_grp gslb_svc_grp_new

stat gslb serviceGroup

Displays configuration statistics of the specified GSLB service group or all the GSLB service groups configured on the appliance.

Synopsis

stat gslb serviceGroup

Arguments

serviceGroupName Name of the GSLB service group for which to display settings.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

State Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)

Service type (Type) The service type of this service.Possible values are ADNS, DNS, MYSQL, RTSP, SSL_DIAMETER, ADNS_TCP, DNS_TCP, NNTP, SIP_UDP, SSL_TCP, ANY, FTP, RADIUS, SNMP, TCP, DHCPRA, HTTP, RDP, SSL, TFTP, DIAMETER, MSSQL, RPCSVR, SSL_BRIDGE, UDP

Related Commands

- stat gslb serviceGroupMember

disable gslb serviceGroup

Disables a GSLB service group or a member of a GSLB service group. To disable a GSLB service group, provide only the service group name. To disable only a member of a service group, in addition to the GSLB service group name, provide the name of the server that hosts the service, and the port number of the service.

Synopsis

disable gslb serviceGroup <serviceGroupName>@

Arguments

serviceGroupName Name of the GSLB service group.

serverName Name of the server that hosts the GSLB service.

port Port number of the GSLB service.

delay The time allowed (in seconds) for a graceful shutdown. During this period, new connections or requests will continue to be sent to this service for clients who already have a persistent session on the system. Connections or requests from fresh or new clients who do not yet have a persistence sessions on the system will not be sent to the service. Instead, they will be load balanced among other available services. After the delay time expires, no new requests or connections will be sent to the service.

graceFul Wait for all existing connections to the service to terminate before shutting down the service.

Possible values: YES, NO Default value: NO

Example

disable gslb servicegroup http_svc_group 10.102.27.153 80 -delay 10

unset gslb serviceGroup

Removes the attributes of the specified GSLB service group. Attributes for which a default value is available revert to their default values..Refer to the set gslb serviceGroup command for meanings of the arguments.

Synopsis

unset gslb serviceGroup <serviceGroupName>@ [(<serverName>@ <port>) | -sitePersistence]

Example

unset gslb servicegroup http_svc_group -maxClient

unbind gslb serviceGroup

Unbinds a service or a monitor from a GSLB service group.

Synopsis

unbind gslb serviceGroup <serviceGroupName> ((<IP>@ <port>) | <serverName>@ | -monitorName <string>@)

Arguments

serviceGroupName Name of the GSLB service group.

IP IP address of the server that hosts the GSLB service. Mutually exclusive with the Server Name parameter.

serverName Name of the server that hosts the service. Mutually exclusive with the IP Address parameter.

port Port number of the GSLB service.

monitorName Name of the monitor to bind to the GSLB service group.

Example

unbind gslb servicegroup http_svc_group 10.102.27.153 80

bind gslb serviceGroup

Binds a service to a GSLB service group.

Synopsis

bind gslb serviceGroup <serviceGroupName> ((<IP>@ <port>) | <serverName>@ | ((-monitorName <string>@) | -state (ENABLED | DISABLED) | -hashId <positive_integer> | | | -publicIP <ip_addr|ipv6_addr|*> | -publicPort <port> | -sitePrefix <string> | -order <positive_integer>))

Arguments

serviceGroupName Name of the GSLB service group.

IP IP address of the server that hosts the GSLB service. Mutually exclusive with the Server Name parameter.

serverName Name of the server that hosts the GSLB service. Mutually exclusive with the IP address parameter.

port Port number of the GSLB service. Each service must have a unique port number.

monitorName The name of the GSLB service or a GSLB service group to which the monitor is to be bound.

monState Administrative state assigned to the monitor and GSLB service group binding. If set to disabled, the service group is not monitored.

Possible values: ENABLED, DISABLED Default value: ENABLED

passive Indicates if load monitor is passive. A passive load monitor does not remove service from LB decision when threshold is breached.

weight When used along with monitor name, it specifies the weight of the monitor binding. When used along with servername & port pair, it specifies the weight of this GSLB service . Default value: 1 Minimum value: 1 Maximum value: 100

state Initial state of the service after binding.

Possible values: ENABLED, DISABLED Default value: ENABLED

hashId Unique numerical identifier used by hash based load balancing methods to identify a service. Minimum value: 1

publicIP The public IP address that a NAT device translates to the GSLB service's private IP address. Optional.

publicPort The public port associated with the GSLB service's public IP address. The port is mapped to the service's private port number. Applicable to the local GSLB service. Optional.

sitePrefix The site's prefix string. When the GSLB service group is bound to a GSLB virtual server, a GSLB site domain is generated internally for each bound serviceitem-domain pair by concatenating the site prefix of the service item and the name of the domain. If the special string NONE is specified, the site-prefix string is unset. When implementing HTTP redirect site persistence, the Citrix ADC redirects GSLB requests to GSLB services by using their site domains.

order Order number to be assigned to the gslb servicegroup member Minimum value: 0

Example

bind gslb servicegroup http_svc_group 10.102.27.153 80

gslb-serviceGroupMember

The following operations can be performed on "gslb-serviceGroupMember":

stat gslb serviceGroupMember

Display statistics of a GSLB service group member.

Synopsis

stat gslb serviceGroupMember <serviceGroupName> (<IP> | <serverName>) <port>

Arguments

serviceGroupName Displays statistics for the specified GSLB service group.Name of the GSLB service group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters.CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my servicegroup" or 'my servicegroup').

IP IP address of the GSLB service group. Mutually exclusive with the server name parameter.

serverName Name of the server. Mutually exclusive with the IP address parameter.

port Port number of the service group member.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Current Client Est connections (ClntEstConn) Number of client connections in ESTABLISHED state.

IP address (IP) The IP address on which the service is running.

Port (port) The port on which the service is running.

Service type (Type) The service type of this service.Possible values are ADNS, DNS, MYSQL, RTSP, SSL_DIAMETER, ADNS_TCP, DNS_TCP, NNTP, SIP_UDP, SSL_TCP, ANY, FTP, RADIUS, SNMP, TCP, DHCPRA, HTTP, RDP, SSL, TFTP, DIAMETER, MSSQL, RPCSVR, SSL_BRIDGE, UDP

State Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)

Service Group Member Binding Order (Order) Order with which service group member is bound to service group

Request bytes (Reqb) Total number of request bytes received on this service or virtual server.

Response bytes (Rspb) Number of response bytes received by this service or virtual server.

Current load on the service (Load) Load on the service that is calculated from the bound load based monitor.

Requests (Req) Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Responses (Rsp) Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Current client connections (ClntConn) Number of current client connections.

Current server connections (SvrConn) Number of current connections to the actual servers behind the virtual server.

Binding Order (Order) Order with which service is bound to vserver

Current Server Est connections (SvrEstConn) Number of server connections in ESTABLISHED state.

Related Commands

- stat gslb domain

gslb-site

The following operations can be performed on "gslb-site":

add| unset| set| rm| stat| show|

add gslb site

Creates a global server load balancing site.

Synopsis

add gslb site <siteName> <siteIPAddress> [-clip <ip_addr|ipv6_addr|*>]

Arguments

siteName Name for the GSLB site. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my gslbsite" or 'my gslbsite').

siteType Type of site to create. If the type is not specified, the appliance automatically detects and sets the type on the basis of the IP address being assigned to the site. If the specified site IP address is owned by the appliance (for example, a MIP address or SNIP address), the site is a local site. Otherwise, it is a remote site.

Possible values: REMOTE, LOCAL Default value: NONE

siteIPAddress IP address for the GSLB site. The GSLB site uses this IP address to communicate with other GSLB sites. For a local site, use any IP address that is owned by the appliance (for example, a SNIP or MIP address, or the IP address of the ADNS service).

publicIP Public IP address for the local site. Required only if the appliance is deployed in a private address space and the site has a public IP address hosted on an external firewall or a NAT device.

metricExchange Exchange metrics with other sites. Metrics are exchanged by using Metric Exchange Protocol (MEP). The appliances in the GSLB setup exchange health information once every second.

If you disable metrics exchange, you can use only static load balancing methods (such as round robin, static proximity, or the hash-based methods), and if you disable metrics exchange when a dynamic load balancing method (such as least connection) is in operation, the appliance falls back to round robin. Also, if you disable metrics exchange, you must use a monitor to determine the state of GSLB services. Otherwise, the service is marked as DOWN.

Possible values: ENABLED, DISABLED Default value: ENABLED

nwMetricExchange Exchange, with other GSLB sites, network metrics such as round-trip time (RTT), learned from communications with various local DNS (LDNS) servers used by clients. RTT information is used in the dynamic RTT load balancing method, and is exchanged every 5 seconds.

Possible values: ENABLED, DISABLED Default value: ENABLED

sessionExchange Exchange persistent session entries with other GSLB sites every five seconds.

Possible values: ENABLED, DISABLED Default value: ENABLED

triggerMonitor Specify the conditions under which the GSLB service must be monitored by a monitor, if one is bound. Available settings function as follows:

- ALWAYS - Monitor the GSLB service at all times.
- MEPDOWN - Monitor the GSLB service only when the exchange of metrics through the Metrics Exchange Protocol (MEP) is disabled. MEPDOWN_SVCDOWN - Monitor the service in either of the following situations:
- The exchange of metrics through MEP is disabled.
- The exchange of metrics through MEP is enabled but the status of the service, learned through metrics exchange, is DOWN.

Possible values: ALWAYS, MEPDOWN, MEPDOWN_SVCDOWN Default value: ALWAYS

parentSite Parent site of the GSLB site, in a parent-child topology.

clip Cluster IP address. Specify this parameter to connect to the remote cluster site for GSLB auto-sync. Note: The cluster IP address is defined when creating the cluster.

publicCLIP IP address to be used to globally access the remote cluster when it is deployed behind a NAT. It can be same as the normal cluster IP address.

naptrReplacementSuffix The naptr replacement suffix configured here will be used to construct the naptr replacement field in NAPTR record.

backupParentlist The list of backup gslb sites configured in preferred order. Need to be parent gsb sites. Default value: "None"

Example

add site new_york LOCAL 192.168.100.12 -publicIP 65.200.211.139

unset gslb site

Use this command to remove gslb site settings.Refer to the set gslb site command for meanings of the arguments.

Synopsis

unset gslb site <siteName>

set gslb site

Modifies the specified parameters of a global server load balancing (GSLB) site.

Synopsis

set gslb site <siteName>

Arguments

siteName Name of the GSLB site.

metricExchange Exchange metrics with other sites. Metrics are exchanged by using Metric Exchange Protocol (MEP). The appliances in the GSLB setup exchange health information once every second.

If you disable metrics exchange, you can use only static load balancing methods (such as round robin, static proximity, or the hash-based methods), and if you disable metrics exchange when a dynamic load balancing method (such as least connection) is in operation, the appliance falls back to round robin. Also, if you disable metrics exchange, you must use a monitor to determine the state of GSLB services. Otherwise, the service is marked as DOWN.

Possible values: ENABLED, DISABLED Default value: ENABLED

nwMetricExchange Exchange, with other GSLB sites, network metrics such as round-trip time (RTT), learned from communications with various local DNS (LDNS) servers used by clients. RTT information is used in the dynamic RTT load balancing method, and is exchanged every 5 seconds.

Possible values: ENABLED, DISABLED Default value: ENABLED

sessionExchange Exchange persistent session entries with other GSLB sites every five seconds.

Possible values: ENABLED, DISABLED Default value: ENABLED

triggerMonitor Specify the conditions under which the GSLB service must be monitored by a monitor, if one is bound. Available settings function as follows:

- ALWAYS - Monitor the GSLB service at all times.
- MEPDOWN - Monitor the GSLB service only when the exchange of metrics through the Metrics Exchange Protocol (MEP) is disabled. MEPDOWN_SVCDOWN - Monitor the service in either of the following situations:
- The exchange of metrics through MEP is disabled.
- The exchange of metrics through MEP is enabled but the status of the service, learned through metrics exchange, is DOWN.

Possible values: ALWAYS, MEPDOWN, MEPDOWN_SVCDOWN Default value: ALWAYS

naptrReplacementSuffix The naptr replacement suffix configured here will be used to construct the naptr replacement field in NAPTR record.

backupParentlist The list of backup gslb sites configured in preferred order. Need to be parent gsb sites. Default value: "None"

Example

set gslb site new_york - metricExchange DISABLED

rm gslb site

Removes a global server load balancing (GSLB) site and all its constituent GSLB services.

Synopsis

rm gslb site <siteName>

Arguments

siteName Name of the GSLB site to remove.

Example

rm gslb site new_york

stat gslb site

Displays statistics for a GSLB site.

Synopsis

stat gslb site

Arguments

siteName Name of the GSLB site for which to display detailed statistics. If a name is not specified, basic information about all GSLB sites is displayed.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Gslb Site Public IP address (Public IP) The public IP address of this GSLB site.

Gslb Site private IP address (Private IP) The private IP address of this GSLB site.

Metric Exchange State (MEPstate) Indicates the status of the Metric Exchange Policy at this GSLB site.

Persistence Exchange (PersMEP) Indicates whether Persistence entries exchange is enabled or disabled at this GSLB site.

Network Metric Exchange (NwMEP) Indicates whether network metric exchange is enabled or disabled at this GSLB site.

Metric Exchange (MEP) Indicates whether metric exchange is enabled or disabled at this GSLB site.

GSLB Site type (sitetype) Indicates whether this GSLB site is local or remote.

Gslb Site private IP address (Private IP) The private IP address of this GSLB site.

Gslb Site public IP address (Public IP) The public IP address of this GSLB site.

Site Metric Metric Exchange State (SiteMetricMEPstate) Indicates the status of the site metric Metric Exchange connection at this GSLB site.

Network Metric Metric Exchange State (NwMetricMEPstate) Indicates the status of the network metric Metric Exchange connection at this GSLB site.

Request bytes (Reqb) Total number of request bytes received by the virtual servers represented by all GSLB services associated with this GSLB site.

Response bytes (Rspb) Number of response bytes received by the virtual servers represented by all GSLB services associated with this GSLB site.

Requests (Req) Total number of requests received by the virtual servers represented by all GSLB services associated with this GSLB site.

Responses (Rsp) Number of responses received by the virtual servers represented by all GSLB services associated with this GSLB site.

Current client connections (ClntConn) Number of current client connections to the virtual servers represented by all GSLB services associated with this GSLB site.

Current server connections (SvrConn) Number of current connections to the real servers behind the virtual servers represented by all GSLB services associated with this GSLB site.

Related Commands

- stat gslb serviceGroupMember

show gslb site

Displays the parameters of all the GSLB sites configured on the appliance, or the parameters of the specified GSLB site.

Synopsis

show gslb site show gslb site stats - alias for 'stat gslb site'

Arguments

siteName Name of the GSLB site. If you specify a site name, details of all the site's constituent services are also displayed.

Output

siteType Specifies whether the site is LOCAL or REMOTE.

siteIPAddress The IP address of the site.

publicIP The Public IP of the gslb site.

metricExchange Exchange metrics with other sites. Metrics are exchanged by using Metric Exchange Protocol (MEP). The appliances in the GSLB setup exchange health information once every second.

If you disable metrics exchange, you can use only static load balancing methods (such as round robin, static proximity, or the hash-based methods), and if you disable metrics exchange when a dynamic load balancing method (such as least connection) is in operation, the appliance falls back to round robin. Also, if you disable metrics exchange, you must use a monitor to determine the state of GSLB services. Otherwise, the service is marked as DOWN.

serviceName Service name.

IPAddress IP Address of the gslb service.

port Port number of the gslb service.

state State of the gslb service.

status Current metric exchange status.

persistenceMEPStatus Network metric and persistence exchange MEP connection status

serviceType Service type.

nwMetricExchange Specifies whether the exchange of network metrics like RTT is enabled or disabled.

sessionExchange Specifies whether the exchange of persistence session entries is enabled or disabled.

triggerMonitor Specify the conditions under which the GSLB service must be monitored by a monitor, if one is bound. Available settings function as follows:

- ALWAYS - Monitor the GSLB service at all times.
- MEPDOWN - Monitor the GSLB service only when the exchange of metrics through the Metrics Exchange Protocol (MEP) is disabled. MEPDOWN_SVCDOWN - Monitor the service in either of the following situations:
- The exchange of metrics through MEP is disabled.
- The exchange of metrics through MEP is enabled but the status of the service, learned through metrics exchange, is DOWN.

parentSite Parent site of the GSLB site, in a parent-child topology.

cnameEntry The cname of the gslb service.

stateflag stateflag

version will be true if the remote site's version is ncore compatible with the local site.(>= 9.2)

clip Cluster IP address. Specify this parameter to connect to the remote cluster site for GSLB auto-sync. Note: The cluster IP address is defined when creating the cluster.

publicCLIP IP address to be used to globally access the remote cluster when it is deployed behind a NAT. It can be same as the normal cluster IP address.

naptrReplacementSuffix The naptr replacement suffix configured here will be used to construct the naptr replacement field in NAPTR record.

backupParentlist The list of backup gslb sites configured in preferred order. Need to be parent gsb sites.

curBackupparentIP Current active backup parent IP address since the configured is DOWN.

serviceGroupName Servicegroup name.

svcitmnum This field is introduced for maintaining service items ordering while displaying gslb service groups

svcgrnm This field is introduced for displaying service groups bound to site.

siteState Site state.

devno count

Example

show site new_york

gslb-syncStatus

The following operations can be performed on "gslb-syncStatus":

show gslb syncStatus

Displays the status of the last GSLB configuration synchronization.

Synopsis

show gslb syncStatus

Arguments

summary sync status summary to be displayed in one line (Success/Failure), in case of Failure stating reason for failure

Output

response gslb sync status as text blob

gslb-vserver

The following operations can be performed on "gslb-vserver":

enable| bind| add| unset| unbind| set| stat| show| rm| disable| rename|

enable gslb vserver

Enables a global server load balancing (GSLB) virtual server that has been disabled. (A GSLB virtual server is enabled by default.)

Synopsis

enable gslb vserver <name>@

Arguments

name Name of the GSLB virtual server to enable.

Example

enable gslb vserver gslb_vip To enable multiple gslb vservers use the following command: enable gslb vserver gslb_vip

bind gslb vserver

Binds a domain, service, backup IP address, or cookie domain to a GSLB virtual server.

Synopsis

bind gslb vserver <name> ((-serviceName <string>) | -serviceGroupName <string>@ | (-domainName <string>) | (-policyName <string>@))

Arguments

name Name of the virtual server on which to perform the binding operation.

serviceName Name of the GSLB service for which to change the weight.

weight Weight to assign to the GSLB service. Default value: 1 Minimum value: 1 Maximum value: 100

serviceGroupName Name of the service group.

domainName Domain name for which to change the time to live (TTL) and/or backup service IP address.

TTL Time to live (TTL) for the domain. Minimum value: 1

backupIP The IP address of the backup service for the specified domain name. Used when all the services bound to the domain are down, or when the backup chain of virtual servers is down.

cookieDomain The cookie domain for the GSLB site. Used when inserting the GSLB site cookie in the HTTP response.

cookieTimeout Timeout, in minutes, for the GSLB site cookie.

sitedomainTTL TTL, in seconds, for all internally created site domains (created when a site prefix is configured on a GSLB service) that are associated with this virtual server. Default value: 3600 Minimum value: 1

policyName Name of the policy bound to the GSLB vserver.

priority Priority. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE. oIf gotoPriorityExpression is not present or if it is equal to END then the policy bank evaluation ends here oElse if the gotoPriorityExpression is equal to NEXT then the next policy in the priority order is evaluated. oElse gotoPriorityExpression

is evaluated. The result of gotoPriorityExpression (which has to be a number) is processed as follows: -An UNDEF event is triggered if .gotoPriorityExpression cannot be evaluated .gotoPriorityExpression evaluates to number which is smaller than the maximum priority in the policy bank but is not same as any policy's priority .gotoPriorityExpression evaluates to a priority that is smaller than the current policy's priority -If the gotoPriorityExpression evaluates to the priority of the current policy then the next policy in the priority order is evaluated. -If the gotoPriorityExpression evaluates to the priority of a policy further ahead in the list then that policy will be evaluated next. This field is applicable only to rewrite and responder policies.

type Bind point to which to bind the policy.

Possible values: REQUEST, RESPONSE, MQTT_JUMBO_REQ

order Order number to be assigned to the service when it is bound to the lb vserver. Minimum value: 1 Maximum value: 8192

Example

bind gslb vserver gvip -domainName www.mynw.com

add gslb vserver

Creates a global server load balancing (GSLB) virtual server.

Synopsis

add gslb vserver <name> <serviceType>

Arguments

name Name for the GSLB virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver').

serviceType Protocol used by services bound to the virtual server.

Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, ANY, SIP_UDP, SIP_TCP, SIP_SSL, RADIUS, RDP, RTSP, MYSQL, MSSQL, ORACLE

dnsRecordType DNS record type to associate with the GSLB virtual server's domain name.

Possible values: A, AAAA, CNAME, NAPTR Default value: A

lbMethod Load balancing method for the GSLB virtual server.

Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT, CUSTOMLOAD, API Default value: LEASTCONNECTION

backupLBMethod Backup load balancing method. Becomes operational if the primary load balancing method fails or cannot be used. Valid only if the primary method is based on either round-trip time (RTT) or static proximity.

Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT, CUSTOMLOAD, API

netmask IPv4 network mask for use in the SOURCEIPHASH load balancing method. Default value: 0xFFFFFFFF

v6netmasklen Number of bits to consider, in an IPv6 source IP address, for creating the hash that is required by the SOURCEIPHASH load balancing method. Default value: 128 Minimum value: 1 Maximum value: 128

rule Expression, or name of a named expression, against which traffic is evaluated. This field is applicable only if gslb method or gslb backup method are set to API. The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Default value: "none"

tolerance Site selection tolerance, in milliseconds, for implementing the RTT load balancing method. If a site's RTT deviates from the lowest RTT by more than the specified tolerance, the site is not considered when the Citrix ADC makes a GSLB decision. The appliance implements the round robin method of global server load balancing between sites whose RTT values are within the specified tolerance. If the tolerance is 0 (zero), the appliance always sends clients the IP address of the site with the lowest RTT. Minimum value: 0 Maximum value: 100

persistenceType Use source IP address based persistence for the virtual server. After the load balancing method selects a service for the first packet, the IP address received in response to the DNS query is used for subsequent requests from the same client.

Possible values: SOURCEIP, NONE

persistenceId The persistence ID for the GSLB virtual server. The ID is a positive integer that enables GSLB sites to identify the GSLB virtual server, and is required if source IP address based or spill over based persistence is enabled on the virtual server. Minimum value: 0 Maximum value: 65535

persistMask The optional IPv4 network mask applied to IPv4 addresses to establish source IP address based persistence. Default value: 0xFFFFFFFF

v6persistmasklen Number of bits to consider in an IPv6 source IP address when creating source IP address based persistence sessions. Default value: 128 Minimum value: 1 Maximum value: 128

timeout Idle time, in minutes, after which a persistence entry is cleared. Default value: 2 Minimum value: 2 Maximum value: 1440

EDR Send clients an empty DNS response when the GSLB virtual server is DOWN.

Possible values: ENABLED, DISABLED Default value: DISABLED

ECS If enabled, respond with EDNS Client Subnet (ECS) option in the response for a DNS query with ECS. The ECS address will be used for persistence and spillover persistence (if enabled) instead of the LDNS address. Persistence mask is ignored if ECS is enabled.

Possible values: ENABLED, DISABLED Default value: DISABLED

ecsAddrValidation Validate if ECS address is a private or unroutable address and in such cases, use the LDNS IP.

Possible values: ENABLED, DISABLED Default value: DISABLED

MIR Include multiple IP addresses in the DNS responses sent to clients.

Possible values: ENABLED, DISABLED Default value: DISABLED

disablePrimaryOnDown Continue to direct traffic to the backup chain even after the primary GSLB virtual server returns to the UP state. Used when spillover is configured for the virtual server.

Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicWeight Specify if the appliance should consider the service count, service weights, or ignore both when using weight-based load balancing methods. The state of the number of services bound to the virtual server help the appliance to select the service.

Possible values: SERVICECOUNT, SERVICEWEIGHT, DISABLED Default value: DISABLED

state State of the GSLB virtual server.

Possible values: ENABLED, DISABLED Default value: ENABLED

considerEffectiveState If the primary state of all bound GSLB services is DOWN, consider the effective states of all the GSLB services, obtained through the Metrics Exchange Protocol (MEP), when determining the state of the GSLB virtual server. To consider the effective state, set the parameter to STATE_ONLY. To disregard the effective state, set the parameter to NONE.

The effective state of a GSLB service is the ability of the corresponding virtual server to serve traffic. The effective state of the load balancing virtual server, which is transferred to the GSLB service, is UP even if only one virtual server in the backup chain of virtual servers is in the UP state.

Possible values: NONE, STATE_ONLY Default value: NONE

comment Any comments that you might want to associate with the GSLB virtual server.

soMethod Type of threshold that, when exceeded, triggers spillover. Available settings function as follows:

- CONNECTION - Spillover occurs when the number of client connections exceeds the threshold.
- DYNAMICCONNECTION - Spillover occurs when the number of client connections at the GSLB virtual server exceeds the sum of the maximum client (Max Clients) settings for bound GSLB services. Do not specify a spillover threshold for this setting, because the threshold is implied by the Max Clients settings of the bound GSLB services.
- BANDWIDTH - Spillover occurs when the bandwidth consumed by the GSLB virtual server's incoming and outgoing traffic exceeds the threshold.
- HEALTH - Spillover occurs when the percentage of weights of the GSLB services that are UP drops below the threshold. For example, if services gslbSvc1, gslbSvc2, and gslbSvc3 are bound to a virtual server, with weights 1, 2, and 3, and the spillover threshold is 50%, spillover occurs if gslbSvc1 and gslbSvc3 or gslbSvc2 and gslbSvc3 transition to DOWN.
- NONE - Spillover does not occur.

Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence If spillover occurs, maintain source IP address based persistence for both primary and backup GSLB virtual servers.

Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeOut Timeout for spillover persistence, in minutes. Default value: 2 Minimum value: 2 Maximum value: 1440

soThreshold Threshold at which spillover occurs. Specify an integer for the CONNECTION spillover method, a bandwidth value in kilobits per second for the BANDWIDTH method (do not enter the units), or a percentage for the HEALTH method (do not enter the percentage symbol). Minimum value: 1 Maximum value: 4294967287

soBackupAction Action to be performed if spillover is to take effect, but no backup chain to spillover is usable or exists

Possible values: DROP, ACCEPT, REDIRECT

appflowLog Enable logging appflow flow information

Possible values: ENABLED, DISABLED Default value: ENABLED

toggleorder Configure this option to toggle order preference

Possible values: ASCENDING, DESCENDING Default value: ASCENDING

orderthreshold This option is used to to specify the threshold of minimum number of services to be UP in an order, for it to be considered in Lb decision. Default value: 0 Minimum value: 0 Maximum value: 100

Example

add gslb vserver gvip http

unset gslb vserver

Removes the specified settings from the specified global server load balancing (GSLB) virtual server. Attributes for which a default value is available revert to their default values..Refer to the set gslb vserver command for meanings of the arguments.

Synopsis

unset gslb vserver <name>@ [-serviceName <string>]

Example

unset gslb vserver lb_vip -backupVServer For multiple gslb vservers the command is: unset gslb vserver lb_vip -backupVServer

unbind gslb vserver

Unbinds the domain or service from the GSLB virtual server.

Synopsis

unbind gslb vserver <name> (-serviceName <string> | -serviceGroupName <string>@ | (-domainName <string>) | -policyName <string>@)

Arguments

name Name of the GSLB virtual server.

serviceName Name of the GSLB service for which to change the weight.

serviceGroupName The name of the service group that is unbound.

domainName Domain name for which to change the time to live (TTL) and/or backup service IP address.

backupIP The IP address of the backup service for the specified domain name. Used when all the services bound to the domain are down, or when the backup chain of virtual servers is down.

cookieDomain The cookie domain for the GSLB site. Used when inserting the GSLB site cookie in the HTTP response.

policyName The policy that has been bound to this load balancing virtual server, using the ###bind gslb vserver### command.

Example

unbind gslb vserver gvip -domainName www.mynw.com

set gslb vserver

Modifies the specified parameters of a global server load balancing (GSLB) virtual server.

Synopsis

set gslb vserver <name> [-serviceName <string>] [-domainName <string>]

Arguments

name Name of the GSLB virtual server.

dnsRecordType DNS record type to associate with the GSLB virtual server's domain name.

Possible values: A, AAAA, CNAME, NAPTR Default value: A

backupVServer Name of the backup GSLB virtual server to which the appliance should to forward requests if the status of the primary GSLB virtual server is down or exceeds its spillover threshold.

lbMethod Load balancing method for the GSLB virtual server.

Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT, CUSTOMLOAD, API Default value: LEASTCONNECTION

backupLBMethod Backup load balancing method. Becomes operational if the primary load balancing method fails or cannot be used. Valid only if the primary method is based on either round-trip time (RTT) or static proximity.

Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT, CUSTOMLOAD, API

netmask IPv4 network mask for use in the SOURCEIPHASH load balancing method. Default value: 0xFFFFFFFF

v6netmasklen Number of bits to consider, in an IPv6 source IP address, for creating the hash that is required by the SOURCEIPHASH load balancing method. Default value: 128 Minimum value: 1 Maximum value: 128

tolerance Site selection tolerance, in milliseconds, for implementing the RTT load balancing method. If a site's RTT deviates from the lowest RTT by more than the specified tolerance, the site is not considered when the Citrix ADC makes a GSLB decision. The appliance implements the round robin method of global server load balancing between sites whose RTT values are within the specified tolerance. If the tolerance is 0 (zero), the appliance always sends clients the IP address of the site with the lowest RTT. Minimum value: 0 Maximum value: 100

persistenceType Persistence type for the virtual server. Possible value for this parameter is SOURCEIP, which specifies persistence based on the source IP address of inbound packets. After

the load balancing method selects a link for transmission of the first packet, the IP address received in response to the DNS query is used for subsequent requests from the same client.

Possible values: SOURCEIP, NONE

persistenceId The persistence ID for the GSLB virtual server. The ID is a positive integer that enables GSLB sites to identify the GSLB virtual server, and is required if source IP address based or spill over based persistence is enabled on the virtual server. Minimum value: 0 Maximum value: 65535

persistMask The optional IPv4 network mask applied to IPv4 addresses to establish source IP address based persistence. Default value: 0xFFFFFFFF

v6persistmasklen Number of bits to consider in an IPv6 source IP address when creating source IP address based persistence sessions. Default value: 128 Minimum value: 1 Maximum value: 128

timeout Idle time, in minutes, after which a persistence entry is cleared. Default value: 2 Minimum value: 2 Maximum value: 1440

EDR Send clients an empty DNS response when the GSLB virtual server is DOWN.

Possible values: ENABLED, DISABLED Default value: DISABLED

ECS If enabled, respond with EDNS Client Subnet (ECS) option in the response for a DNS query with ECS. The ECS address will be used for persistence and spillover persistence (if enabled) instead of the LDNS address. Persistence mask is ignored if ECS is enabled.

Possible values: ENABLED, DISABLED Default value: DISABLED

ecsAddrValidation Validate if ECS address is a private or unroutable address and in such cases, use the LDNS IP.

Possible values: ENABLED, DISABLED Default value: DISABLED

MIR Include multiple IP addresses in the DNS responses sent to clients.

Possible values: ENABLED, DISABLED Default value: DISABLED

disablePrimaryOnDown Continue to direct traffic to the backup chain even after the primary GSLB virtual server returns to the UP state. Used when spillover is configured for the virtual server.

Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicWeight Specify if the appliance should consider the service count, service weights, or ignore both when using weight-based load balancing methods. The state of the number of services bound to the virtual server help the appliance to select the service.

Possible values: SERVICECOUNT, SERVICEWEIGHT, DISABLED Default value: DISABLED

considerEffectiveState If the primary state of all bound GSLB services is DOWN, consider the effective states of all the GSLB services, obtained through the Metrics Exchange Protocol (MEP), when determining the state of the GSLB virtual server. To consider the effective state, set the parameter to STATE_ONLY. To disregard the effective state, set the parameter to NONE.

The effective state of a GSLB service is the ability of the corresponding virtual server to serve traffic. The effective state of the load balancing virtual server, which is transferred to the GSLB service, is UP even if only one virtual server in the backup chain of virtual servers is in the UP state.

Possible values: NONE, STATE_ONLY Default value: NONE

soMethod Type of threshold that, when exceeded, triggers spillover. Available settings function as follows:

- CONNECTION - Spillover occurs when the number of client connections exceeds the threshold.
- DYNAMICCONNECTION - Spillover occurs when the number of client connections at the GSLB virtual server exceeds the sum of the maximum client (Max Clients) settings for bound GSLB services. Do not specify a spillover threshold for this setting, because the threshold is implied by the Max Clients settings of the bound GSLB services.
- BANDWIDTH - Spillover occurs when the bandwidth consumed by the GSLB virtual server's incoming and outgoing traffic exceeds the threshold.
- HEALTH - Spillover occurs when the percentage of weights of the GSLB services that are UP drops below the threshold. For example, if services gslbSvc1, gslbSvc2, and gslbSvc3 are bound to a virtual server, with weights 1, 2, and 3, and the spillover threshold is 50%, spillover occurs if gslbSvc1 and gslbSvc3 or gslbSvc2 and gslbSvc3 transition to DOWN.
- NONE - Spillover does not occur.

Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence If spillover occurs, maintain source IP address based persistence for both primary and backup GSLB virtual servers.

Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeOut Timeout for spillover persistence, in minutes. Default value: 2 Minimum value: 2 Maximum value: 1440

soThreshold Threshold at which spillover occurs. Specify an integer for the CONNECTION spillover method, a bandwidth value in kilobits per second for the BANDWIDTH method (do not enter the units), or a percentage for the HEALTH method (do not enter the percentage symbol). Minimum value: 1 Maximum value: 4294967287

soBackupAction Action to be performed if spillover is to take effect, but no backup chain to spillover is usable or exists

Possible values: DROP, ACCEPT, REDIRECT

serviceName Name of the GSLB service for which to change the weight.

weight Weight for the service. Minimum value: 1 Maximum value: 100

serviceGroupName The GSLB service group name bound to the selected GSLB virtual server.

domainName Domain name for which to change the time to live (TTL) and/or backup service IP address.

TTL Time to live (TTL) for the domain. Minimum value: 1

backupIP The IP address of the backup service for the specified domain name. Used when all the services bound to the domain are down, or when the backup chain of virtual servers is down.

cookieDomain The cookie domain for the GSLB site. Used when inserting the GSLB site cookie in the HTTP response.

cookieTimeout Timeout, in minutes, for the GSLB site cookie. Maximum value: 1440

sitedomainTTL TTL, in seconds, for all internally created site domains (created when a site prefix is configured on a GSLB service) that are associated with this virtual server. Minimum value: 1

comment Any comments that you might want to associate with the GSLB virtual server.

appflowLog Enable logging appflow flow information

Possible values: ENABLED, DISABLED Default value: ENABLED

rule Expression, or name of a named expression, against which traffic is evaluated. This field is applicable only if gslb method or gslb backup method are set to API. The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Default value: "none"

toggleorder Configure this option to toggle order preference

Possible values: ASCENDING, DESCENDING Default value: ASCENDING

orderthreshold This option is used to to specify the threshold of minimum number of services to be UP in an order, for it to be considered in Lb decision. Default value: 0 Minimum value: 0 Maximum value: 100

order Order number to be assigned to the service when it is bound to the lb vserver. Minimum value: 1 Maximum value: 8192

Example

set gslb vserver gvip -persistenceType SOURCEIP

stat gslb vserver

Displays statistics associated with a global server load balancing (GSLB) virtual server.

Synopsis

stat gslb vserver

Arguments

name Name of the GSLB virtual server for which to display statistics. If you do not specify a name, statistics are displayed for all GSLB virtual servers.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Current Client Est connections (ClntEstConn) Number of client connections in ESTABLISHED state.

total INACTIVE services (inactSvcs) number of INACTIVE services bound to a vserver

Vserver Health (Health) Health of the vserver. This gives percentage of UP services bound to this vserver.

Vserver protocol (Protocol) Protocol associated with the vserver

State Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)

total ACTIVE services (actSvcs) number of ACTIVE services bound to a vserver

Vserver hits (Hits) Total vserver hits

Primary LB Method Failures (Backup LB Hits) Total backup LB method hits

Backup LB Method Failures (Backup LB Fail) Total backup LB method fails

Current Persistence Sessions (PersistenceSessions) current vserver owned persistence sessions

Vserver Persistence Hits (Total Vserver Persistence Hits) Total number of Persistence hits at vserver

Request bytes (Reqb) Total number of request bytes received on this service or virtual server.

Response bytes (Rspb) Number of response bytes received by this service or virtual server.

Spill Over Threshold (SOThresh) Spill Over Threshold set on the VServer.

Spill Over Hits (NumSo) Number of times vserver experienced spill over.

Vserver Down Backup Hits (VserverDownBackupHits) Number of times traffic was diverted to backup vserver since primary vserver was DOWN.

Requests (Req) Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Responses (Rsp) Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Current client connections (ClntConn) Number of current client connections.

Current server connections (SvrConn) Number of current connections to the actual servers behind the virtual server.

Current Server Est connections (SvrEstConn) Number of server connections in ESTABLISHED state.

Related Commands

- stat gslb serviceGroupMember

show gslb vserver

Displays the parameters of all the global server load balancing (GSLB) virtual servers configured on the appliance, or the parameters of the specified GSLB virtual server.

Synopsis

show gslb vserver show gslb vserver stats - alias for 'stat gslb vserver'

Arguments

name Name of the GSLB virtual server.

Output

serviceType Protocol used by services bound to the virtual server.

state State of the GSLB virtual server.

ipType The IP type for this GSLB vserver.

dnsRecordType The IP type for this GSLB vserver.

persistenceType Indicates if persistence is set on the gslb vserver

persistenceId Persistence id of the gslb vserver

lbMethod The load balancing method set for the virtual server

backupLBMethod Indicates the backup method in case the primary fails

tolerance Indicates the deviation we can tolerate when we have the LB method as RTT

timeout Idle timeout for persistence entries.

state State of the gslb vserver.

netmask The netmask used in the SOURCEIPHASH policy.

v6netmasklen The netmask used for ipv6 traffic in the SOURCE/DEST IPHASH policy.

persistMask The netmask used while SOURCEIP based persistency is ENABLED.

v6persistmasklen The netmask applied for ipv6 traffic when the persistency type is SOURCEIP.

serviceName The service name.

weight Weight for the service.

domainName The name of the domain for which TTL and/or backupIP has changed.

TTL TTL for the given domain.

backupIP Backup IP for the given domain.

cookieDomain The cookie domain for the GSLB domain. This will be used when inserting the GSLB site cookie in the HTTP response. By default, cookie domain will not be inserted.

cookieTimeout Time out value of the cookie in minutes

sitedomainTTL Site domain TTL.

IPAddress IP address.

port Port number.

status Current status of the gslb vserver. During the initial phase if the configured lb method is not round robin , the vserver will adopt round robin to distribute traffic for a predefined number of requests.

lbrrreason Reason why a vserver is in RR. The following are the reasons: 1 - MEP is DOWN (GSLB) 2 - LB method has changed 3 - Bound service's state changed to UP 4 - A new service is bound 5 - Startup RR factor has changed 6 - LB feature is enabled 7 - Load monitor is not active on a service 8 - Vserver is Enabled 9 - SSL feature is Enabled 10 - All bound services have reached threshold. Using effective state to load balance (GSLB) 11 - Primary state of bound services are not UP. Using effective state to load balance (GSLB) 12 - No LB decision can be made as all bound services have either reached threshold or are not UP (GSLB) 13 - All load monitors are active

preferredLocation The target site to be returned in the DNS response when a policy is successfully evaluated against the incoming DNS request. Target site is specified in dotted notation with up to 6 qualifiers. Wildcard `*' is accepted as a valid qualifier token.

backupVServer Backup vserver in case the primary fails

backupSessionTimeout A non zero value enables the feature. The minimum value is 2 minutes. To disable the feature set the value to zero. The created session is in effect for a specific client per domain.

EDR Indicates if Empty Down Response is enabled/disabled

ECS If enabled, respond with EDNS Client Subnet (ECS) option in the response for a DNS query with ECS. The ECS address will be used for persistence and spillover persistence (if enabled) instead of the LDNS address. Persistence mask is ignored if ECS is enabled.

ecsAddrValidation Validate if ECS address is a private or unroutable address and in such cases, use the LDNS IP.

MIR Indicates if Multi IP Response is enabled/disabled

disablePrimaryOnDown Continue to direct traffic to the backup chain even after the primary GSLB virtual server returns to the UP state. Used when spillover is configured for the virtual server.

dynamicWeight Dynamic weight method. Possible values are, the svc count or the svc weights or ignore both.

isCname is cname feature set on vserver

cumulativeWeight Cumulative weight is the weight of GSLB service considering both its configured weight and dynamic weight. It is equal to product of dynamic weight and configured weight of the gslb service

dynamicConfWt Weight obtained by the virtue of bound service count or weight

thresholdValue Tells whether threshold exceeded for this service participating in CUSTOMLB

sitePersistence Type of Site Persistence set

svrEffGslbState Effective state of the gslb svc

gslbthreshold Indicates if gslb svc has reached threshold

considerEffectiveState If the primary state of all bound GSLB services is DOWN, consider the effective states of all the GSLB services, obtained through the Metrics Exchange Protocol (MEP), when determining the state of the GSLB virtual server. To consider the effective state, set the parameter to STATE_ONLY. To disregard the effective state, set the parameter to NONE.

The effective state of a GSLB service is the ability of the corresponding virtual server to serve traffic. The effective state of the load balancing virtual server, which is transferred to the GSLB service, is UP even if only one virtual server in the backup chain of virtual servers is in the UP state.

cnameEntry The cname of the gslb service.

totalServices Total number of services bound to the vserver.

activeServices Total number of active services bound to the vserver.

stateChangeTimeSec Time when last state change happened. Seconds part.

stateChangeTimemSec Time at which last state change happened. Milliseconds part.

ticksSinceLastStateChange Time in 10 millisecond ticks since the last state change.

comment Any comments that you might want to associate with the GSLB virtual server.

soPersistenceTimeOut Timeout for spillover persistence, in minutes.

soMethod Type of threshold that, when exceeded, triggers spillover. Available settings function as follows:

- CONNECTION - Spillover occurs when the number of client connections exceeds the threshold.

- DYNAMICCONNECTION - Spillover occurs when the number of client connections at the GSLB virtual server exceeds the sum of the maximum client (Max Clients) settings for bound GSLB services. Do not specify a spillover threshold for this setting, because the threshold is implied by the Max Clients settings of the bound GSLB services.
- BANDWIDTH - Spillover occurs when the bandwidth consumed by the GSLB virtual server's incoming and outgoing traffic exceeds the threshold.
- HEALTH - Spillover occurs when the percentage of weights of the GSLB services that are UP drops below the threshold. For example, if services gslbSvc1, gslbSvc2, and gslbSvc3 are bound to a virtual server, with weights 1, 2, and 3, and the spillover threshold is 50%, spillover occurs if gslbSvc1 and gslbSvc3 or gslbSvc2 and gslbSvc3 transition to DOWN.
- NONE - Spillover does not occur.

soBackupAction Action to be performed if spillover is to take effect, but no backup chain to spillover is usable or exists

soPersistence If spillover occurs, maintain source IP address based persistence for both primary and backup GSLB virtual servers.

soThreshold Threshold at which spillover occurs. Specify an integer for the CONNECTION spillover method, a bandwidth value in kilobits per second for the BANDWIDTH method (do not enter the units), or a percentage for the HEALTH method (do not enter the percentage symbol).

health Health of vserver based on percentage of weights of active svcs/all svcs. This does not consider administratively disabled svcs

stateflag stateflag

appflowLog Enable logging appflow flow information

policyName Name of the policy bound to the GSLB vserver.

priority Priority.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE. oIf gotoPriorityExpression is not present or if it is equal to END then the policy bank evaluation ends here oElse if the gotoPriorityExpression is equal to NEXT then the next policy in the priority order is evaluated. oElse gotoPriorityExpression is evaluated. The result of gotoPriorityExpression (which has to be a number) is processed as follows: -An UNDEF event is triggered if .gotoPriorityExpression cannot be evaluated .gotoPriorityExpression evaluates to number which is smaller than the maximum priority

in the policy bank but is not same as any policy's priority .gotoPriorityExpression evaluates to a priority that is smaller than the current policy's priority -If the gotoPriorityExpression evaluates to the priority of the current policy then the next policy in the priority order is evaluated. -If the gotoPriorityExpression evaluates to the priority of a policy further ahead in the list then that policy will be evaluated next. This field is applicable only to rewrite and responder policies.

type The bindpoint to which the policy is bound

vsvrbindsvcip used for showing the ip of bound entities

vsvrbindsvcport used for showing ports of bound entities

gslbBoundSvcType Protocol used by services bound to the GSLBvirtual server.

sitePersistCookie This field is introduced for displaying the cookie in cluster setup.

svcSitePersistence Type of Site Persistence set on the bound service

svcitmnum This field is introduced for maintaining service items ordering while displaying gslb service groups

svcgrnm This field is introduced for displaying service groups bound to vserver.

serverName This field is used to display server name in case of GSLB servicegroup binding to GSLB vserver

serviceGroupName The GSLB service group name bound to the selected GSLB virtual server.

noDefaultBindings to determine if the configuration will have default ssl CIPHER and ECC curve bindings

rule Rule type

order Order number to be assigned to the service when it is bound to the lb vserver.

order Order number in string form assigned to the service when it is bound to the lb vserver.

toggleorder Configure this option to toggle order preference

orderthreshold This option is used to to specify the threshold of minimum number of services to be UP in an order, for it to be considered in Lb decision.

CurrentActiveOrder current order that takes the traffic in case service or servicegroup is bound with order

devno count

Example

show gslb vserver gvip

rm gslb vserver

Removes a global server load balancing (GSLB) virtual server configured on the appliance.

Synopsis

rm gslb vserver <name>

Arguments

name Name of the GSLB virtual server to remove.

Example

rm gslb vserver gvip

disable gslb vserver

Disables a global server load balancing (GSLB) virtual server and takes it out of service.

Synopsis

disable gslb vserver <name>@

Arguments

name Name of the GSLB virtual server to disable.

Example

disable gslb vserver gslb_vip To disable multiple gslb vservers use the following command: disable gslb vserver gslb_vip

rename gslb vserver

Renames a global server load balancing (GSLB) virtual server.

Synopsis

rename gslb vserver <name>@ <newName>@

Arguments

name Existing name of the GSLB virtual server.

newName New name for the GSLB virtual server.

Example

rename gslb vserver gsl_vsvr gslb_vsvr_new

ha

HA-failover

The following operations can be performed on "HA-failover":

force HA failover

Forces an HA failover. Can be initiated from either node. A forced failover is not propagated or synchronized., Note: This command fails under any of the following conditions:

- The secondary node is disabled or configured to remain secondary.
- The primary node is configured to remain primary.
- The state of the peer node is unknown.
- You run the command on a standalone appliance.

Synopsis

force HA failover

Arguments

force Force a failover without prompting for confirmation.

HA-files

The following operations can be performed on "HA-files":

sync HA files

Synchronize various configuration files from the primary node to the secondary. You can run this command from either node. Files that are present on only the secondary and are specific to the secondary are not deleted. This command fails if the secondary node is disabled, the secondary node is not accessible from the primary, or you enter the command on a standalone appliance.

Synopsis

sync HA files

Arguments

Mode Specify one of the following modes of synchronization.

- all - Synchronize files related to system configuration, Access Gateway bookmarks, SSL certificates, SSL CRL lists, and Application Firewall XML objects.
- bookmarks - Synchronize all Access Gateway bookmarks.
- ssl - Synchronize all certificates, keys, and CRLs for the SSL feature.
- imports. Synchronize all XML objects (for example, WSDLs, schemas, error pages) configured for the application firewall.
- misc - Synchronize all license files and the rc.conf file.
- all_plus_misc - Synchronize files related to system configuration, Access Gateway bookmarks, SSL certificates, SSL CRL lists, application firewall XML objects, licenses, and the rc.conf file.

Example

sync files all

HA-node

The following operations can be performed on "HA-node":

show| rm| unset| set| unbind| add| bind| stat|

show HA node

Displays the HA settings of both nodes or, if you specify a node, just the specified node. You can use this command to display the master state (primary or secondary) of the nodes in a HA configuration.

Synopsis

show HA node

Arguments

id ID of the node whose HA settings you want to display. (The ID of the local node is always 0.) Minimum value: 0 Maximum value: 64

Output

name Node Name.

IPAddress IP Address of the node.

flags The flags for this entry.

stateflag haStatus HA status.

state HA Master State.

haSync HA Sync State.

haProp HA Propagation Status.

enaifaces Enabled interfaces.

disifaces Disabled interfaces.

hamonifaces HAMON ON interfaces.

haHeartbeatifaces HAHEARTBEAT OFF interfaces.

pfifaces Interfaces causing Partial Failure.

ifaces Interfaces on which non-multicast is not seen.

netmask The netmask.

inc INC state.

ssl2 SSL card status.

helloInterval Hello Interval.

deadInterval Dead Interval.

masterStateTime Time elapsed in current master state

failSafe Keep one node primary if both nodes fail the health check, so that a partially available node can back up data and handle traffic. This mode is set independently on each node.

routeMonitor The IP address (IPv4 or IPv6).

maxFlips Max number of flips allowed before becoming sticky primary

maxFlipTime Interval after which flipping of node states can again start

curFlips Keeps track of number of flips that have happened till now in current interval

completedFlipTime To inform user whether flip time is elapsed or not

syncvlan Vlan on which HA related communication is sent. This include sync, propagation , connection mirroring , LB persistency config sync, persistent session sync and session state sync. However HA heartbeats can go all interfaces.

routeMonitorState State for route monitor

haSyncFailureReason Displays the reason for HA SYNC Failure

syncStatusStrictmode strict mode flag for sync status

devno count

Example

An example of the command's output is as follows: 2 configured nodes:

1. Node ID: 0 IP: 192.168.100.5 Primary node
2. Node ID: 2 IP: 192.168.100.112 Secondary node

rm HA node

Removes the peer node from the HA configuration. To completely remove both the nodes from the HA configuration, you have to log on to each node and remove its peer node.

Synopsis

rm HA node <id>

Arguments

id Number that uniquely identifies the peer node.

CLI users: To learn the ID of the peer node, run the show HA node command on the local node. Minimum value: 0 Maximum value: 64

unset HA node

Use this command to remove HA node settings.Refer to the set HA node command for meanings of the arguments.

Synopsis

unset HA node

set HA node

Sets the specified HA related parameters for the node. The settings are neither propagated nor synchronized to the peer node.

Synopsis

set HA node

Arguments

haStatus The HA status of the node. The HA status STAYSECONDARY is used to force the secondary device stay as secondary independent of the state of the Primary device. For example, in an existing HA setup, the Primary node has to be upgraded and this process would take few seconds. During the upgradation, it is possible that the Primary node may suffer from a downtime for a few seconds. However, the Secondary should not take over as the Primary node. Thus, the Secondary node should remain as Secondary even if there is a failure in the Primary node. STAYPRIMARY configuration keeps the node in primary state in case if it is healthy, even if the peer node was the primary node initially. If the node with STAYPRIMARY setting (and no peer node) is added to a primary node (which has this node as the peer) then this node takes over as the new primary and the older node becomes secondary. ENABLED state means normal HA operation without any constraints/preferences. DISABLED state disables the normal HA operation of the node.

Possible values: ENABLED, STAYSECONDARY, DISABLED, STAYPRIMARY

haSync Automatically maintain synchronization by duplicating the configuration of the primary node on the secondary node. This setting is not propagated. Automatic synchronization requires that this setting be enabled (the default) on the current secondary node. Synchronization uses TCP port 3010.

Possible values: ENABLED, DISABLED Default value: ENABLED

haProp Automatically propagate all commands from the primary to the secondary node, except the following:

- All HA configuration related commands. For example, add ha node, set ha node, and bind ha node.
- All Interface related commands. For example, set interface and unset interface.
- All channels related commands. For example, add channel, set channel, and bind channel. The propagated command is executed on the secondary node before it is executed on the primary. If command propagation fails, or if command execution fails on the secondary, the primary

node executes the command and logs an error. Command propagation uses port 3010. Note: After enabling propagation, run force synchronization on either node.

Possible values: ENABLED, DISABLED Default value: ENABLED

helloInterval Interval, in milliseconds, between heartbeat messages sent to the peer node. The heartbeat messages are UDP packets sent to port 3003 of the peer node. Default value: 200 Minimum value: 200 Maximum value: 1000

deadInterval Number of seconds after which a peer node is marked DOWN if heartbeat messages are not received from the peer node. Default value: 3 Minimum value: 3 Maximum value: 60

failSafe Keep one node primary if both nodes fail the health check, so that a partially available node can back up data and handle traffic. This mode is set independently on each node.

Possible values: ON, OFF Default value: OFF

maxFlips Max number of flips allowed before becoming sticky primary Default value: 0 Minimum value: 0

maxFlipTime Interval after which flipping of node states can again start Default value: 0 Minimum value: 0

syncvlan Vlan on which HA related communication is sent. This include sync, propagation , connection mirroring , LB persistency config sync, persistent session sync and session state sync. However HA heartbeats can go all interfaces. Minimum value: 1 Maximum value: 4094

syncStatusStrictmode strict mode flag for sync status

Possible values: ENABLED, DISABLED Default value: DISABLED

unbind HA node

Removes a route monitor entry from the local node. The Citrix ADC stops monitoring the route in its internal routing table.

Synopsis

unbind HA node (-routeMonitor <ip_addr|ipv6_addr|*>)

Arguments

id Number that uniquely identifies the local node. The ID of the local node is always 0. Minimum value: 0 Maximum value: 64

routeMonitor The route specified in the route monitor entry that you want to remove from the Citrix ADC. Can be an IPv4 address or network, or an IPv6 address or network prefix.

netmask Subnet mask associated with the IPv4 route specified by the routeMonitor parameter.

add HA node

Adds a peer node to an HA configuration. Each node must add the other as a peer. An algorithm determines which node becomes primary and which becomes secondary.

Synopsis

add HA node <id> <IPAddress>

Arguments

id Number that uniquely identifies the node. For self node, it will always be 0. Peer node values can range from 1-64. Minimum value: 1 Maximum value: 64

IPAddress The NSIP or NSIP6 address of the node to be added for an HA configuration. This setting is neither propagated nor synchronized.

inc This option is required if the HA nodes reside on different networks. When this mode is enabled, the following independent network entities and configurations are neither propagated nor synced to the other node: MIPs, SNIPs, VLANs, routes (except LLB routes), route monitors, RNAT rules (except any RNAT rule with a VIP as the NAT IP), and dynamic routing configurations. They are maintained independently on each node.

Possible values: ENABLED, DISABLED Default value: DISABLED

bind HA node

Adds a route monitor to the local node. When a Citrix ADC has only static routes for reaching a network, and you want to create a route monitor for the network, you must enable monitored static routes (MSR) for the static routes. Route Monitors are supported both in non-INC and INC modes.

Synopsis

bind HA node (-routeMonitor <ip_addr|ipv6_addr|*>)

Arguments

id Number that uniquely identifies the local node. The ID of the local node is always 0. Minimum value: 0 Maximum value: 64

routeMonitor A route that you want the Citrix ADC to monitor in its internal routing table. You can specify an IPv4 address or network, or an IPv6 address or network prefix. If you specify an IPv4 network address or IPv6 network prefix, the appliance monitors any route that matches the network or prefix.

netmask Subnet mask associated with the IPv4 route specified by the routeMonitor parameter.

stat HA node

Display the statistics related to HA configuration.

Synopsis

stat HA node

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

High Availability (HA) Whether a Citrix ADC is configured for high availability. Possible values are YES and NO. If the value is NO, the high availability statistics below are invalid.

System state (HAState) State of the HA node, based on its health, in a high availability setup. Possible values are: UP - Indicates that the node is accessible and can function as either a primary or secondary node. DISABLED - Indicates that the high availability status of the node has been manually disabled. Synchronization and propagation cannot take place between the peer nodes. INIT - Indicates that the node is in the process of becoming part of the high availability

configuration. PARTIALFAIL - Indicates that one of the high availability monitored interfaces has failed because of a card or link failure. This state triggers a failover. COMPLETEFAIL - Indicates that all the interfaces of the node are unusable, because the interfaces on which high availability monitoring is enabled are not connected or are manually disabled. This state triggers a failover. DUMB - Indicates that the node is in listening mode. It does not participate in high availability transitions or transfer configuration from the peer node. This is a configured value, not a statistic. PARTIALFAILSSL - Indicates that the SSL card has failed. This state triggers a failover. ROUTEMONITORFAIL - Indicates that the route monitor has failed. This state triggers a failover.

Master state (mastate) Indicates the high availability state of the node. Possible values are: STAYSECONDARY - Indicates that the selected node remains the secondary node in a high availability setup. In this case a forced failover does not change the state but, instead, returns an appropriate error message. This is a configured value and not a statistic. PRIMARY - Indicates that the selected node is the primary node in a high availability setup. SECONDARY - Indicates that the selected node is the secondary node in a high availability setup. CLAIMING - Indicates that the secondary node is in the process of taking over as the primary node. This is the intermediate state in the transition of the secondary node to primary status. FORCE CHANGE - Indicates that the secondary node is forcibly changing its status to primary due to a forced failover issued on the secondary node.

Last Transition time (TransTime) Time when the last master state transition occurred. You can use this statistic for debugging.

Heartbeats received (HApktrx) Number of heartbeat packets received from the peer node. Heartbeats are sent at regular intervals (default is 200 milliseconds) to determine the state of the peer node.

Heartbeats sent (HApkttx) Number of heartbeat packets sent to the peer node. Heartbeats are sent at regular intervals (default is 200 milliseconds) to determine the state of the peer node.

Propagation timeouts (ptimeout) Number of times propagation timed out.

Sync failure (syncfail) Number of times the configuration of the primary and secondary nodes failed to synchronize since that last transition. A synchronization failure results in mismatched configuration. It can be caused by a mismatch in the Remote Procedural Call (RPC) password on the two nodes forming the high availability pair.

HA-sync

The following operations can be performed on "HA-sync":

force HA sync

Forces duplication of the primary node's configuration on the secondary node. Can be executed from either node. Note: This command fails under any of the following conditions:

- Synchronization is already in progress.
- The secondary node is disabled.
- Synchronization is disabled on either node
- The secondary node is not accessible from the primary.
- You run the command on a standalone appliance.

Synopsis

force HA sync [-force]

Arguments

force Force synchronization regardless of the state of HA propagation and HA synchronization on either node.

save After synchronization, automatically save the configuration in the secondary node configuration file (ns.conf) without prompting for confirmation.

Possible values: YES, NO Default value: VAL_NOT_SET

Example

Can be used in following formats:

```
force sync <cr> force sync -force <cr> force sync -force -save <cr>
```

HA-syncFailures

The following operations can be performed on "HA-syncFailures":

show HA syncFailures

Displays the list of commands failed during HA configuration synchronization.

Synopsis

show HA syncFailures

Output

response Displays the list of commands failed during HA configuration synchronization.

Example

show ha syncFailures

Ha

The entities on which you can perform NetScaler CLI operations:

- HA-failover
- HA-files
- HA-node
- HA-sync
- HA-syncFailures

ica

ica-accessprofile

The following operations can be performed on "ica-accessprofile":

unset| show| add| set| rm|

unset ica accessprofile

Use this command to remove ica accessprofile settings.Refer to the set ica accessprofile command for meanings of the arguments.

Synopsis

unset ica accessprofile <name>

show ica accessprofile

Displays details of the specified ica accessprofile. If no accessprofile is specified, displays a list of ica accessprofiles on the Citrix ADC.

Synopsis

show ica accessprofile

Arguments

name Name of the ica accessprofile.

Output

stateflag ConnectClientLPTPorts Allow Default access/Disable automatic connection of LPT ports from the client when the user logs on

ClientAudioRedirection Allow Default access/Disable applications hosted on the server to play sounds through a sound device installed on the client computer, also allows or prevents users to record audio input

LocalRemoteDataSharing Allow Default access/Disable file/data sharing via the Receiver for HTML5

ClientClipboardRedirection Allow Default access/Disable the clipboard on the client device to be mapped to the clipboard on the server

ClientCOMPortRedirection Allow Default access/Disable COM port redirection to and from the client

ClientDriveRedirection Allow Default access/Disables drive redirection to and from the client

ClientPrinterRedirection Allow Default access/Disable client printers to be mapped to a server when a user logs on to a session

Multistream Allow Default access/Disable the multistream feature for the specified users

ClientUSBDriveRedirection Allow Default access/Disable the redirection of USB devices to and from the client

refCnt Number of entities using this accessprofile

builtin Indicates that the ICA accessprofile is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

isDefault A value of true is returned if it is a default accessprofile

devno count

Example

sh ica accessprofile profile1

add ica accessprofile

This command creates an ica accessprofile that specifies status of the features (DEFAULT/ DISABLED).

Synopsis

add ica accessprofile <name>

Arguments

name Name for the ICA accessprofile. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the ICA accessprofile is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my ica accessprofile" or 'my ica accessprofile').

Each of the features can be configured as DEFAULT/DISABLED. Here, DISABLED means that the policy settings on the backend XenApp/XenDesktop server are overridden and the Citrix ADC makes the decision to deny access. Whereas DEFAULT means that the Citrix ADC allows the request to reach the XenApp/XenDesktop that takes the decision to allow/deny access based on the policy configured on it. For example, if ClientAudioRedirection is enabled on the backend XenApp/XenDesktop server, and the configured profile has ClientAudioRedirection as DISABLED, the Citrix ADC makes the decision to deny the request irrespective of the configuration on the backend. If the configured profile has ClientAudioRedirection as DEFAULT, then the Citrix ADC forwards the requests to the backend XenApp/XenDesktop server.It then makes the decision to allow/deny access based on the policy configured on it.

ConnectClientLPTPorts Allow Default access/Disable automatic connection of LPT ports from the client when the user logs on

Possible values: DEFAULT, DISABLED Default value: DISABLED

ClientAudioRedirection Allow Default access/Disable applications hosted on the server to play sounds through a sound device installed on the client computer, also allows or prevents users to record audio input

Possible values: DEFAULT, DISABLED Default value: DISABLED

LocalRemoteDataSharing Allow Default access/Disable file/data sharing via the Receiver for HTML5

Possible values: DEFAULT, DISABLED Default value: DISABLED

ClientClipboardRedirection Allow Default access/Disable the clipboard on the client device to be mapped to the clipboard on the server

Possible values: DEFAULT, DISABLED Default value: DISABLED

ClientCOMPortRedirection Allow Default access/Disable COM port redirection to and from the client

Possible values: DEFAULT, DISABLED Default value: DISABLED

ClientDriveRedirection Allow Default access/Disables drive redirection to and from the client

Possible values: DEFAULT, DISABLED Default value: DISABLED

ClientPrinterRedirection Allow Default access/Disable client printers to be mapped to a server when a user logs on to a session

Possible values: DEFAULT, DISABLED Default value: DISABLED

Multistream Allow Default access/Disable the multistream feature for the specified users

Possible values: DEFAULT, DISABLED Default value: DISABLED

ClientUSBDriveRedirection Allow Default access/Disable the redirection of USB devices to and from the client

Possible values: DEFAULT, DISABLED Default value: DISABLED

Example

add ica accessprofile profile1 -ClientAudioRedirection DISABLED

set ica accessprofile

This command modifies the specified parameters of the specified ica accessprofile.

Synopsis

set ica accessprofile <name>

Arguments

name Name of the profile that you want to modify.

ConnectClientLPTPorts Allow Default access/Disable automatic connection of LPT ports from the client when the user logs on

Possible values: DEFAULT, DISABLED Default value: DISABLED

ClientAudioRedirection Allow Default access/Disable applications hosted on the server to play sounds through a sound device installed on the client computer, also allows or prevents users to record audio input

Possible values: DEFAULT, DISABLED Default value: DISABLED

LocalRemoteDataSharing Allow Default access/Disable file/data sharing via the Receiver for HTML5

Possible values: DEFAULT, DISABLED Default value: DISABLED

ClientClipboardRedirection Allow Default access/Disable the clipboard on the client device to be mapped to the clipboard on the server

Possible values: DEFAULT, DISABLED Default value: DISABLED

ClientCOMPortRedirection Allow Default access/Disable COM port redirection to and from the client

Possible values: DEFAULT, DISABLED Default value: DISABLED

ClientDriveRedirection Allow Default access/Disables drive redirection to and from the client

Possible values: DEFAULT, DISABLED Default value: DISABLED

ClientPrinterRedirection Allow Default access/Disable client printers to be mapped to a server when a user logs on to a session

Possible values: DEFAULT, DISABLED Default value: DISABLED

Multistream Allow Default access/Disable the multistream feature for the specified users

Possible values: DEFAULT, DISABLED Default value: DISABLED

ClientUSBDriveRedirection Allow Default access/Disable the redirection of USB devices to and from the client

Possible values: DEFAULT, DISABLED Default value: DISABLED

Example

set ica accessprofile profile1 -ClientAudioRedirection DEFAULT

rm ica accessprofile

This command removes the specified ica accessprofile.

Synopsis

rm ica accessprofile <name>

Arguments

name Name of the ICA accessprofile.

Example

rm ica accessprofile profile1

ica-action

The following operations can be performed on "ica-action":

set| show| add| rename| rm| unset|

set ica action

This command modifies the specified parameters of the specified ica action.

Synopsis

set ica action <name>

Arguments

name Name of the action that you want to modify.

accessProfileName Name of the ica accessprofile to be associated with this action.

latencyprofileName Name of the ica latencyprofile to be associated with this action.

Example

set ica action ica_action_1 -accessprofileName profile2

show ica action

This command displays details of the specified ica action. If no profile is specified, displays a list of ica actions on the Citrix ADC.

Synopsis

show ica action

Arguments

name Name of the ICA action.

Output

stateflag accessProfileName Name of the ica accessprofile to be associated with this action.

latencyprofileName Name of the ica latencyprofile to be associated with this action.

hits The number of times the action has been taken.

referenceCount The number of references to the action.

undefHits The number of times the action resulted in UNDEF.

builtin Indicates that the ICA action is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

isDefault A value of true is returned if it is a default action

devno count

Example

sh ica action ica_action_1

add ica action

Creates an ICA action, which is used to specify the ICA accessprofile.The action can be associated with an ICA policy by using the add ica policy command

Synopsis

add ica action <name>

Arguments

name Name for the ICA action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the ICA action is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my ica action" or 'my ica action').

accessProfileName Name of the ica accessprofile to be associated with this action.

latencyprofileName Name of the ica latencyprofile to be associated with this action.

Example

add ica action ica_action_1 -accessprofileName profile1

rename ica action

This command renames an ICA action.

Synopsis

rename ica action <name>@ <newName>@

Arguments

name Name of the existing action.

newName New name for the ICA action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#),period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my ica action" or 'my ica action').

Example

rename ica action old_name new_name

rm ica action

This command removes the ica action specified

Synopsis

rm ica action <name>

Arguments

name Name of the action to be removed.

Example

rm ica action ica_action_1

unset ica action

Use this command to remove ica action settings.Refer to the set ica action command for meanings of the arguments.

Synopsis

unset ica action <name>

Ica

The entities on which you can perform NetScaler CLI operations:

- ica-accessprofile
- ica-action
- ica-global
- ica-latencyprofile
- ica-parameter
- ica-policy

ica-global

The following operations can be performed on "ica-global":

show| unbind| bind|

show ica global

Displays the ICA global bind points and the number of policies bound to each global bind point, or more detailed information about the specified bind point.

Synopsis

show ica global

Arguments

type Global bind point for which to show detailed information about the policies bound to the bind point.

Possible values: ICA_REQ_OVERRIDE, ICA_REQ_DEFAULT

Output

stateflag policyName Name of the ICA policy.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

numpol The number of policies bound to the bindpoint.

flowType Flow type of the bound ICA policy.

flags globalBindType devno count

Example

show ica global

unbind ica global

Unbinds entities from an ICA global bind point.

Synopsis

unbind ica global (-policyName <string>)

Arguments

policyName Name of the policy to be unbound.

type Bind point from which to unbind the policy.

Possible values: ICA_REQ_OVERRIDE, ICA_REQ_DEFAULT

priority Priority of the NOPOLICY to be unbound. Applicable only if a NOPOLICY has been bound to the bind point. Minimum value: 1 Maximum value: 2147483647

Example

unbind ica global -policyName pol9

bind ica global

This command binds the ICA policy to one of the two global lists of ICA policies. A policy becomes active only after it is bound.

Synopsis

bind ica global -policyName <string> -priority <positive_integer>

Arguments

policyName Name of the ICA policy to be bound.

priority Integer specifying the priority of the policy. The lower the number, the higher the priority. By default, policies in the list are evaluated in the order of their priority numbers. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the priority of the next policy, within the policy list, to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher numbered priority.
- END - Stop evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy list. If the final goto in the invoked policy list has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy list performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, it's evaluation result determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, that policy is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher priority number is evaluated next.
- If the expression evaluates to a priority number that is numerically higher than the highest priority number, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

type The bind point to which to bind the policy.

Possible values: ICA_REQ_OVERRIDE, ICA_REQ_DEFAULT

Example

i bind ica global -policyName pol9 -priority 9

ica-latencyprofile

The following operations can be performed on "ica-latencyprofile":

show| rm| add| unset| set|

show ica latencyprofile

Displays details of the specified ica l7latencyprofile. If no l7latencyprofile is specified, displays a list of ica l7latencyprofiles on the Citrix ADC.

Synopsis

show ica latencyprofile

Arguments

name Name of the ica l7latencyprofile.

Output

stateflag l7LatencyMonitoring Enable/Disable L7 Latency monitoring for L7 latency notifications

l7LatencyThresholdFactor L7 Latency threshold factor. This is the factor by which the active latency should be greater than the minimum observed value to determine that the latency is high and may need to be reported

l7LatencyWaitTime L7 Latency Wait time. This is the time for which the Citrix ADC waits after the threshold is exceeded before it sends out a Notification to the Insight Center.

l7LatencyNotifyInterval L7 Latency Notify Interval. This is the interval at which the Citrix ADC sends out notifications to the Insight Center after the wait time has passed.

l7LatencyMaxNotifyCount L7 Latency Max notify Count. This is the upper limit on the number of notifications sent to the Insight Center within an interval where the Latency is above the threshold.

refCnt Number of entities using this l7latencyprofile

builtin Indicates that the ICA latencyprofile is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

isDefault A value of true is returned if it is a default l7latencyprofile

devno count

Example

sh ica l7latencyprofile profile1

rm ica latencyprofile

This command removes the specified ica l7latencyprofile.

Synopsis

rm ica latencyprofile <name>

Arguments

name Name of the ICA l7latencyprofile.

Example

rm ica l7latencyprofile profile1

add ica latencyprofile

This command creates an ica latencyprofile with the options specified.

Synopsis

add ica latencyprofile <name>

Arguments

name Name for the ICA latencyprofile. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the ICA latency profile is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my ica l7latencyprofile" or 'my ica l7latencyprofile').

l7LatencyMonitoring Enable/Disable L7 Latency monitoring for L7 latency notifications

Possible values: ENABLED, DISABLED Default value: DISABLED

l7LatencyThresholdFactor L7 Latency threshold factor. This is the factor by which the active latency should be greater than the minimum observed value to determine that the latency is high and may need to be reported Default value: 4 Minimum value: 2 Maximum value: 65535

l7LatencyWaitTime L7 Latency Wait time. This is the time for which the Citrix ADC waits after the threshold is exceeded before it sends out a Notification to the Insight Center. Default value: 20 Minimum value: 1 Maximum value: 65535

l7LatencyNotifyInterval L7 Latency Notify Interval. This is the interval at which the Citrix ADC sends out notifications to the Insight Center after the wait time has passed. Default value: 20 Minimum value: 1 Maximum value: 65535

l7LatencyMaxNotifyCount L7 Latency Max notify Count. This is the upper limit on the number of notifications sent to the Insight Center within an interval where the Latency is above the threshold. Default value: 5 Minimum value: 1 Maximum value: 65535

Example

add ica latencyprofile profile1 -l7latencythresholdfactor 4

unset ica latencyprofile

Use this command to remove ica latencyprofile settings.Refer to the set ica latencyprofile command for meanings of the arguments.

Synopsis

unset ica latencyprofile <name>

set ica latencyprofile

This command modifies the specified parameters of the specified ica l7latencyprofile.

Synopsis

set ica latencyprofile <name>

Arguments

name Name of the profile that you want to modify.

l7LatencyMonitoring Enable/Disable L7 Latency monitoring for L7 latency notifications

Possible values: ENABLED, DISABLED Default value: DISABLED

l7LatencyThresholdFactor L7 Latency threshold factor. This is the factor by which the active latency should be greater than the minimum observed value to determine that the latency is high and may need to be reported Default value: 4 Minimum value: 2 Maximum value: 65535

l7LatencyWaitTime L7 Latency Wait time. This is the time for which the Citrix ADC waits after the threshold is exceeded before it sends out a Notification to the Insight Center. Default value: 20 Minimum value: 1 Maximum value: 65535

l7LatencyNotifyInterval L7 Latency Notify Interval. This is the interval at which the Citrix ADC sends out notifications to the Insight Center after the wait time has passed. Default value: 20 Minimum value: 1 Maximum value: 65535

l7LatencyMaxNotifyCount L7 Latency Max notify Count. This is the upper limit on the number of notifications sent to the Insight Center within an interval where the Latency is above the threshold. Default value: 5 Minimum value: 1 Maximum value: 65535

Example

set ica l7latencyprofile profile1 -latencyThresholdfactor 20

ica-parameter

The following operations can be performed on "ica-parameter":

unset| show| set|

unset ica parameter

Use this command to remove ica parameter settings.Refer to the set ica parameter command for meanings of the arguments.

Synopsis

unset ica parameter

show ica parameter

Displays the global ica configuration

Synopsis

show ica parameter

Arguments

Output

EnableSRonHAFailover Enable/Disable Session Reliability on HA failover. The default value is No

HDXInsightNonNSAP Enable/Disable HDXInsight for Non NSAP ICA Sessions. The default value is Yes

EDTPmtudDF Enable/Disable DF enforcement for EDT PMTUD Control Blocks

EDTPmtudDFTimeout DF enforcement timeout for EDTPMTUDDF

builtin Indicates that the ICA parameter is a built-in (SYSTEM INTERNAL) type.

L7LatencyFrequency Specify the time interval/period for which L7 Client Latency value is to be calculated. By default, L7 Client Latency is calculated for every packet. The default value is 0

Example

show ica parameter

set ica parameter

Sets the global ica configuration parameter

Synopsis

set ica parameter

Arguments

EnableSRonHAFailover Enable/Disable Session Reliability on HA failover. The default value is No

Possible values: YES, NO Default value: NO

HDXInsightNonNSAP Enable/Disable HDXInsight for Non NSAP ICA Sessions. The default value is Yes

Possible values: YES, NO Default value: YES

EDTPmtudDF Enable/Disable DF enforcement for EDT PMTUD Control Blocks

Possible values: ENABLED, DISABLED Default value: ENABLED

EDTPmtudDFTimeout DF enforcement timeout for EDTPMTUDDF Default value: 100 Minimum value: 10 Maximum value: 65535

L7LatencyFrequency Specify the time interval/period for which L7 Client Latency value is to be calculated. By default, L7 Client Latency is calculated for every packet. The default value is 0 Default value: 0 Minimum value: 0 Maximum value: 60

Example

set ica parameter -EnableSRonHAFailover YES

ica-policy

The following operations can be performed on "ica-policy":

add| rm| unset| stat| show| set| rename|

add ica policy

This command adds an ICA policy. The policy specifies the rule, on which the traffic is evaluated, and the action to be taken if the rule returns "TRUE".

Synopsis

add ica policy <name> -rule <expression> -action <string>

Arguments

name Name for the policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my ica policy" or 'my ica policy').

rule Expression or other value against which the traffic is evaluated. Must be a Boolean expression.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the ica action to be associated with this policy.

comment Any type of information about this ICA policy.

logAction Name of the messagelog action to use for requests that match this policy.

Example

add ica policy <name> -rule <expression> -action <string> , where the action is the ica action name

rm ica policy

This command removes an ICA policy

Synopsis

rm ica policy <name>

Arguments

name Name of the policy to be removed.

Example

rm ica policy ica_policy_1

unset ica policy

Use this command to remove ica policy settings.Refer to the set ica policy command for meanings of the arguments.

Synopsis

unset ica policy <name>

stat ica policy

Displays statistics for the specified ICA policy. If no policy name is specified, displays abbreviated statistics for all ICA policies currently configured on the Citrix ADC.

Synopsis

stat ica policy

Arguments

name Name of the ica policy.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Policy undef hits (Undefhits) Number of undef hits on the policy

Example

stat ica policy

show ica policy

This command displays information about all configured ICA policies, or detailed information about the specified policy.

Synopsis

show ica policy show ica policy stats - alias for 'stat ica policy'

Arguments

name Name of the policy about which to display detailed information.

Output

stateflag rule Expression to be used by ICA policy.

action ICA profile (action) associated with the policy.

hits Number of hits.

undefHits Number of policy UNDEF hits.

activePolicy Indicates whether policy is bound or not.

comment Any type of information about this ICA policy.

logAction Name of the messagelog action to use for requests that match this policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

boundTo Location where policy is bound.

priority Specifies the priority of the policy.

bindPolicyType vserverType builtin Indicates that the ICA policy is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

type devno count

Example

show ica policy

set ica policy

This command modifies the parameters like rule, action , comment etc for an existing ICA policy.

Synopsis

set ica policy <name>

Arguments

name Name of the policy to modify.

rule Expression or other value against which the traffic is evaluated. Must be a Boolean expression.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.

- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the ica action to be associated with this policy.

comment Any type of information about this ICA policy.

logAction Name of the messagelog action to use for requests that match this policy.

Example

set ica policy ica_policy -rule <rule>

rename ica policy

This command renames an ICA policy.

Synopsis

rename ica policy <name>@ <newName>@

Arguments

name Existing name of the policy.

newName New name for the policy. Must begin with an ASCII alphabetic or underscore (_)character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), s pace, colon (:), at (@), equals (=), and hyphen (-) characters.

The following requirement applies only to the Citrix ADC CLI:

If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my ica policy" or 'my ica policy').

Example

rename ica policy old_name new_name

ipsec

Ipsec

The entities on which you can perform NetScaler CLI operations:

- ipsec-counters
- ipsec-parameter
- ipsec-profile

ipsec-counters

The following operations can be performed on "ipsec-counters":

stat ipsec counters

Display statistics for secure tunnel sessions.

Synopsis

stat ipsec counters

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Bytes Received (ipsecRxBytes) Bytes received during IPsec sessions.

Bytes Sent (ipsecTxBytes) Bytes sent during IPsec sessions.

Packets Received (ipsecRxPkts) Packets received during IPsec sessions.

Packets Sent (ipsecTxPkts) Packets sent during IPsec sessions.

Example

stat ipsec

ipsec-parameter

The following operations can be performed on "ipsec-parameter":

show| set| unset|

show ipsec parameter

Show global parameters for IPSEC

Synopsis

show ipsec parameter

Arguments

Output

ikeVersion IKE Protocol Version

encAlgo Type of encryption algorithm (Note: Selection of AES enables AES128)

hashAlgo Type of hashing algorithm

lifetime Lifetime of IKE SA in seconds. Lifetime of IPSec SA will be (lifetime of IKE SA/8)

livenessCheckInterval Number of seconds after which a notify payload is sent to check the liveliness of the peer. Additional retries are done as per retransmit interval setting. Zero value disables liveliness checks.

replayWindowSize IPSec Replay window size for the data traffic

ikeRetryInterval IKE retry interval for bringing up the connection

perfectForwardSecrecy Enable/Disable PFS.

responderOnly Responder Only config for IKED.

retransmissiontime The interval in seconds to retry sending the IKE messages to peer, three consecutive attempts are done with doubled interval after every failure, increases for every retransmit till 6 retransmits.

set ipsec parameter

Set global parameters for IPSEC

Synopsis

set ipsec parameter

Arguments

ikeVersion IKE Protocol Version

Possible values: V1, V2 Default value: V2

encAlgo Type of encryption algorithm (Note: Selection of AES enables AES128) Default value: AES

hashAlgo Type of hashing algorithm Default value: HMAC_SHA256

lifetime Lifetime of IKE SA in seconds. Lifetime of IPSec SA will be (lifetime of IKE SA/8) Minimum value: 480 Maximum value: 31536000

livenessCheckInterval Number of seconds after which a notify payload is sent to check the liveliness of the peer. Additional retries are done as per retransmit interval setting. Zero value disables liveliness checks. Minimum value: 0 Maximum value: 64999

replayWindowSize IPSec Replay window size for the data traffic Minimum value: 0 Maximum value: 16384

ikeRetryInterval IKE retry interval for bringing up the connection Minimum value: 60 Maximum value: 3600

perfectForwardSecrecy Enable/Disable PFS.

Possible values: ENABLE, DISABLE Default value: DISABLE

retransmissiontime The interval in seconds to retry sending the IKE messages to peer, three consecutive attempts are done with doubled interval after every failure, increases for every retransmit till 6 retransmits. Minimum value: 1 Maximum value: 99

unset ipsec parameter

Set global parameters for IPSEC.Refer to the set ipsec parameter command for meanings of the arguments.

Synopsis

unset ipsec parameter

ipsec-profile

The following operations can be performed on "ipsec-profile":

rm| add| show|

rm ipsec profile

Remove an ipsec peer

Synopsis

rm ipsec profile <name>

Arguments

name The name of the ipsec profile.

Example

rm ipsec profile

add ipsec profile

Add an ipsec profile.

Synopsis

add ipsec profile <name> (-psk | (-publickey <string> -privatekey <string> -peerPublicKey <string>))

Arguments

name The name of the ipsec profile

ikeVersion IKE Protocol Version

Possible values: V1, V2

encAlgo Type of encryption algorithm (Note: Selection of AES enables AES128)

hashAlgo Type of hashing algorithm

lifetime Lifetime of IKE SA in seconds. Lifetime of IPSec SA will be (lifetime of IKE SA/8) Minimum value: 480 Maximum value: 31536000

psk Pre shared key value

publickey Public key file path

privatekey Private key file path

peerPublicKey Peer public key file path

livenessCheckInterval Number of seconds after which a notify payload is sent to check the liveliness of the peer. Additional retries are done as per retransmit interval setting. Zero value disables liveliness checks. Minimum value: 0 Maximum value: 64999

replayWindowSize IPSec Replay window size for the data traffic Minimum value: 0 Maximum value: 16384

ikeRetryInterval IKE retry interval for bringing up the connection Minimum value: 60 Maximum value: 3600

retransmissiontime The interval in seconds to retry sending the IKE messages to peer, three consecutive attempts are done with doubled interval after every failure. Minimum value: 1 Maximum value: 99

perfectForwardSecrecy Enable/Disable PFS.

Possible values: ENABLE, DISABLE

show ipsec profile

Display all of the configured ipsec peers

Synopsis

show ipsec profile

Arguments

name The name of the ipsec profile

Output

ikeVersion IKE Protocol Version

encAlgo Type of encryption algorithm.

hashAlgo Type of hashing algorithm

lifetime Lifetime of IKE SA in seconds. Lifetime of IPSec SA will be (lifetime of IKE SA/8)

livenessCheckInterval Number of seconds after which a notify payload is sent to check the liveliness of the peer. Additional retries are done as per retransmit interval setting. Zero value disables liveliness checks.

replayWindowSize IPSec Replay window size for the data traffic

retransmissiontime The interval in seconds to retry sending the IKE messages to peer, three consecutive attempts are done with doubled interval after every failure.

psk Pre shared key value

publickey Public key file path

privatekey Private key file path

peerPublicKey Peer public key file path

ikeRetryInterval IKE retry interval for bringing up the connection

perfectForwardSecrecy Enable/Disable PFS.

responderOnly Responder Only config for IKED.

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

devno count stateflag

Example

show ipsec profile

ipsecalg

Ipsecalg

The entities on which you can perform NetScaler CLI operations:

- ipsecalg-counters
- ipsecalg-profile
- ipsecalg-session

ipsecalg-counters

The following operations can be performed on "ipsecalg-counters":

stat ipsecalg counters

Display statistics for ipsec alg.

Synopsis

stat ipsecalg counters

Arguments

name Name of IPSec ALG Profile.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Total Sessions (Total) Total session for IPSec ALG.

Dropped Sessions (Dropped) Total Dropped IPsec ALG sessions.

Active Sessions (Active) Currently active IPsec ALG sessions.

Blocked Sessions (Blocked) Currently blocked sessions on ESP Gate.

Packets Received (RxPkts) Total Packets received during IPsec ALG sessions.

Packets Sent (TxPkts) Total Packets sent during IPsec ALG sessions.

Example

stat ipsecalg counters

ipsecalg-profile

The following operations can be performed on "ipsecalg-profile":

show| rm| set| unset| add|

show ipsecalg profile

Display all of the configured ipsec alg profiles

Synopsis

show ipsecalg profile

Arguments

name The name of the ipsec alg profile

Output

ikeSessionTimeout IKE session timeout in minutes

espSessionTimeout ESP session timeout in minutes.

espGateTimeout Timeout ESP in seconds as no ESP packets are seen after IKE negotiation

connfailover Mode in which the connection failover feature must operate for the IPSec Alg. After a failover, established UDP connections and ESP packet flows are kept active and resumed on the secondary appliance. Recomended setting is ENABLED.

devno count stateflag

Example

show ipsecalg profile

rm ipsecalg profile

Remove an ipsec alg profile

Synopsis

rm ipsecalg profile <name>

Arguments

name The name of the ipsec alg profile.

Example

rm ipsecalg profile

set ipsecalg profile

Set an ipsec alg profile parameter.

Synopsis

set ipsecalg profile <name>

Arguments

name The name of the ipsec alg profile

ikeSessionTimeout IKE session timeout in minutes Default value: 60 Minimum value: 1 Maximum value: 1440

espSessionTimeout ESP session timeout in minutes. Default value: 60 Minimum value: 1 Maximum value: 1440

espGateTimeout Timeout ESP in seconds as no ESP packets are seen after IKE negotiation Default value: 30 Minimum value: 3 Maximum value: 1200

connfailover Mode in which the connection failover feature must operate for the IPSec Alg. After a failover, established UDP connections and ESP packet flows are kept active and resumed on the secondary appliance. Recomended setting is ENABLED.

Possible values: ENABLED, DISABLED Default value: ENABLED

unset ipsecalg profile

Use this command to remove ipsecalg profile settings.Refer to the set ipsecalg profile command for meanings of the arguments.

Synopsis

unset ipsecalg profile <name>

add ipsecalg profile

Add an ipsec alg profile.

Synopsis

add ipsecalg profile <name>

Arguments

name The name of the ipsec alg profile

ikeSessionTimeout IKE session timeout in minutes Default value: 60 Minimum value: 1 Maximum value: 1440

espSessionTimeout ESP session timeout in minutes. Default value: 60 Minimum value: 1 Maximum value: 1440

espGateTimeout Timeout ESP in seconds as no ESP packets are seen after IKE negotiation Default value: 30 Minimum value: 3 Maximum value: 1200

connfailover Mode in which the connection failover feature must operate for the IPSec Alg. After a failover, established UDP connections and ESP packet flows are kept active and resumed on the secondary appliance. Recomended setting is ENABLED.

Possible values: ENABLED, DISABLED Default value: ENABLED

ipsecalg-session

The following operations can be performed on "ipsecalg-session":

show| flush|

show ipsecalg session

Display all of the configured ipsec alg profiles

Synopsis

show ipsecalg session

Arguments

sourceIP Original Source IP address

natIP Natted Source IP address

destIP Destination IP address

Output

sourceIP Original Source IP address

natIP Natted Source IP address

destIP Destination IP address

spiIn Client SPI for ESP

spiOut Server SPI for ESP

devno count stateflag

Example

show ipsecalg session

flush ipsecalg session

Flush IPSec Alg Sessions

Synopsis

flush ipsecalg session

Arguments

sourceIP Original Source IP address

natIP Natted Source IP address

destIP Destination IP address

Example

flush ipsecalg session

lb

lb-action

The following operations can be performed on "lb-action":

unset| show| set| add| rm| rename|

unset lb action

Use this command to remove lb action settings.Refer to the set lb action command for meanings of the arguments.

Synopsis

unset lb action <name> -comment

show lb action

Displays the current settings for the specified LB action. If no action name is provided, displays a list of all LB actions currently configured on the Citrix ADC, with abbreviated settings.

Synopsis

show lb action

Arguments

name Name for the LB action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb action" or 'my lb action').

Output

stateflag type Type of an LB action. Available settings function as follows:

- NOLBACTION - Does not consider LB action in making LB decision.

- SELECTIONORDER - services bound to vserver with order specified in value parameter is considerd for lb/gslb decision.

value The selection order list used during lb/gslb decision. Preference of services during lb/gslb decision is as follows - services corresponding to first order specified in the sequence is considered first, services corresponding to second order specified in the sequence is considered next and so on. For example, if -value 2 1 3 is specified here and service-1 bound to a vserver with order 1, service-2 bound to a vserver with order 2 and service-3 bound to a vserver with order 3. Then preference of selecting services in LB decision is as follows: service-2, service-1, service-3.

hits The number of times the action has been taken.

referenceCount The number of references to the action.

undefHits The number of times the action resulted in UNDEF.

comment Comment. Any type of information about this LB action.

feature The feature to be checked while applying this config

builtin Flag to determine whether LB action is built-in or not

gslbBindings Number of times action is used in a policy bound to a gslb vserver

devno count

Example

show lb action lbact1

set lb action

Modifies the specified parameters of an LB action.

Synopsis

set lb action <name>

Arguments

name Name for the LB action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb action" or 'my lb action').

value The selection order list used during lb/gslb decision. Preference of services during lb/gslb decision is as follows - services corresponding to first order specified in the sequence is considered first, services corresponding to second order specified in the sequence is considered next and so on. For example, if -value 2 1 3 is specified here and service-1 bound to a vserver with order 1, service-2 bound to a vserver with order 2 and service-3 bound to a vserver with order 3. Then preference of selecting services in LB decision is as follows: service-2, service-1, service-3. Minimum value: 1

comment Comment. Any type of information about this LB action.

Example

set lb action lbact1 -value 3 2 1

add lb action

Creates an LB action which specifies a selection order for the given client request.

Synopsis

add lb action <name> -type (NOLBACTION | SELECTIONORDER)

Arguments

name Name for the LB action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb action" or 'my lb action').

type Type of an LB action. Available settings function as follows:

- NOLBACTION - Does not consider LB action in making LB decision.
- SELECTIONORDER - services bound to vserver with order specified in value parameter is considerd for lb/gslb decision.

Possible values: NOLBACTION, SELECTIONORDER

value The selection order list used during lb/gslb decision. Preference of services during lb/gslb decision is as follows - services corresponding to first order specified in the sequence is considered first, services corresponding to second order specified in the sequence is considered next and so on. For example, if -value 2 1 3 is specified here and service-1 bound to a vserver with order 1, service-2 bound to a vserver with order 2 and service-3 bound to a vserver with order 3. Then preference of selecting services in LB decision is as follows: service-2, service-1, service-3. Minimum value: 1

comment Comment. Any type of information about this LB action.

Example

add lb action lbact1 -type SELECTIONORDER -value 2 1 3

rm lb action

Removes the specified LB action.

Synopsis

rm lb action <name>

Arguments

name Name for the LB action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb action" or 'my lb action').

Example

rm lb action lbact1

rename lb action

Renames an LB action.

Synopsis

rename lb action <name>@ <newName>@

Arguments

name Existing name of the LB action

newName New name for the LB action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb action" or my lb action').

Example

rename lb action lbact1 lbact2

Lb

The entities on which you can perform NetScaler CLI operations:

- lb-action
- lb-global
- lb-group
- lb-metricTable
- lb-monbindings
- lb-monitor
- lb-parameter
- lb-persistentSessions
- lb-policy
- lb-policylabel
- lb-profile
- lb-route
- lb-route6
- lb-sipParameters
- lb-vserver
- lb-wlm

lb-global

The following operations can be performed on "lb-global":

bind| unbind| show|

bind lb global

Activates the specified LB policy for all requests sent to the Citrix ADC.

Synopsis

bind lb global -policyName <string> -priority <positive_integer>

Arguments

policyName Name of the LB policy to activate. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy" or 'my lb policy').

priority Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Must be unique within the label. Policies are evaluated in the order of their priority numbers, and the first policy that matches the request is applied. Minimum value: 1 Maximum value: 2147483647

type Bind point to which to bind the policy. Available settings function as follows:

- REQ_OVERRIDE - Request override. Binds the policy to the override queue.
- REQ_DEFAULT - Binds the policy to the default queue.
- OTHERTCP_REQ_OVERRIDE - Binds the policy to the non-HTTP TCP override queue.
- OTHERTCP_REQ_DEFAULT - Binds the policy to the non-HTTP TCP default queue.
- SIPUDP_REQ_OVERRIDE - Binds the policy to the SIP UDP override queue.
- SIPUDP_REQ_DEFAULT - Binds the policy to the SIP UDP default queue.
- RADIUS_REQ_OVERRIDE - Binds the policy to the RADIUS override queue.
- RADIUS_REQ_DEFAULT - Binds the policy to the RADIUS default queue.
- MSSQL_REQ_OVERRIDE - Binds the policy to the Microsoft SQL override queue.

- MSSQL_REQ_DEFAULT - Binds the policy to the Microsoft SQL default queue.
- MYSQL_REQ_OVERRIDE - Binds the policy to the MySQL override queue.
- MYSQL_REQ_DEFAULT - Binds the policy to the MySQL default queue.
- ORACLE_REQ_OVERRIDE - Binds the policy to the Oracle override queue.
- ORACLE_REQ_DEFAULT - Binds the policy to the Oracle default queue.
- NAT_REQ_OVERRIDE - Binds the policy to the NAT override queue.
- NAT_REQ_DEFAULT - Binds the policy to the NAT default queue.
- DIAMETER_REQ_OVERRIDE - Binds the policy to the Diameter override queue.
- DIAMETER_REQ_DEFAULT - Binds the policy to the Diameter default queue.
- MQTT_REQ_OVERRIDE - Binds the policy to the MQTT override queue.
- MQTT_REQ_DEFAULT - Binds the policy to the MQTT default queue.
- QUIC_OVERRIDE - Binds the policy to the QUIC override queue.
- QUIC_DEFAULT - Binds the policy to the QUIC default queue.
- HTTPQUIC_REQ_OVERRIDE - Binds the policy to the HTTP_QUIC override queue.
- HTTPQUIC_REQ_DEFAULT - Binds the policy to the HTTP_QUIC default queue.
- GSLB_REQ_OVERRIDE- Binds the policy to the GSLB override queue.
- GSLB_REQ_DEFAULT - Binds the policy to the GSLB default queue.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, SIPUDP_REQ_OVERRIDE, SIPUDP_REQ_DEFAULT, SIPTCP_REQ_OVERRIDE, SIPTCP_REQ_DEFAULT, MSSQL_REQ_OVERRIDE, MSSQL_REQ_DEFAULT, MYSQL_REQ_OVERRIDE, MYSQL_REQ_DEFAULT, ORACLE_REQ_OVERRIDE, ORACLE_REQ_DEFAULT, NAT_REQ_OVERRIDE, NAT_REQ_DEFAULT, DIAMETER_REQ_OVERRIDE, DIAMETER_REQ_DEFAULT, RADIUS_REQ_OVERRIDE, RADIUS_REQ_DEFAULT, DNS_REQ_OVERRIDE, DNS_REQ_DEFAULT, MQTT_REQ_OVERRIDE, MQTT_REQ_DEFAULT, QUIC_OVERRIDE, QUIC_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, GSLB_REQ_OVERRIDE, GSLB_REQ_DEFAULT

gotoPriorityExpression Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.

- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.
- The expression evaluates to a priority number that is smaller than the current policy's priority number.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

labelType Type of invocation, Available settings function as follows:

- vserver - Invokes the unnamed policy label associated with the specified virtual server.
- policylabel - Invoke the specified policy label.

Possible values: reqvserver, policylabel

labelName Name of the virtual server or user-defined policy label to invoke if the policy evaluates to TRUE.

Example

bind LB global lbpol1 10

unbind lb global

Unbind the specified LB policy from LB global.

Synopsis

unbind lb global -policyName <string>

Arguments

policyName Name of the policy to unbind.

type The bindpoint from which the policy is to be unbound.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, SIPUDP_REQ_OVERRIDE, SIPUDP_REQ_DEFAULT, SIPTCP_REQ_OVERRIDE, SIPTCP_REQ_DEFAULT, MSSQL_REQ_OVERRIDE, MSSQL_REQ_DEFAULT, MYSQL_REQ_OVERRIDE, MYSQL_REQ_DEFAULT, ORACLE_REQ_OVERRIDE, ORACLE_REQ_DEFAULT, NAT_REQ_OVERRIDE, NAT_REQ_DEFAULT, DIAMETER_REQ_OVERRIDE, DIAMETER_REQ_DEFAULT, RADIUS_REQ_OVERRIDE, RADIUS_REQ_DEFAULT, DNS_REQ_OVERRIDE, DNS_REQ_DEFAULT, MQTT_REQ_OVERRIDE, MQTT_REQ_DEFAULT, QUIC_OVERRIDE, QUIC_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, GSLB_REQ_OVERRIDE, GSLB_REQ_DEFAULT

Example

unbind lb global pol9

show lb global

Displays the list of policies bound to the specified LB global bind point. If no bind point is specified, displays a list of all policies bound to LB global.

Synopsis

show lb global

Arguments

type

Output

stateflag policyName Name of the LB policy.

priority Specifies the priority of the policy.

flowType flowtype of the bound LB policy.

numpol number of polices bound to label.

flags gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

labelType Type of invocation, Available settings function as follows:

- vserver - Invokes the unnamed policy label associated with the specified virtual server.
- policylabel - Invoke the specified policy label.

labelName Name of the virtual server or user-defined policy label to invoke if the policy evaluates to TRUE.

globalBindType devno count

Example

show lb global

lb-group

The following operations can be performed on "lb-group":

unbind| bind| set| show| rm| unset| rename| add|

unbind lb group

Unbinds one or more virtual servers from a group.

Synopsis

unbind lb group <name> <vServerName>@ ...

Arguments

name Name of the load balancing virtual server group.

vServerName Name of the virtual server to unbind. Multiple names can be specified.

Example

unbind lb group webgroup http_vip To unbind multiple vservers use the following command: unbind lb group webgroup v

bind lb group

Binds one or more virtual servers to a load balancing virtual server group. If the specified group does not exist, the Citrix ADC first creates the group, and then binds the virtual servers to it. A virtual server group enables you to specify common persistence settings for all of its members through a single set lb group command. Only address-based virtual servers can be added to a group. Content-based virtual servers (content switching and cache redirection virtual servers) cannot be added. A virtual server can be assigned to only one group at any given time. To move a virtual server from one group to another, the virtual server must first be unbound from the group to which it belongs.

Synopsis

bind lb group <name>@ <vServerName>@ ...

Arguments

name Name for the load balancing virtual server group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lbgroup" or 'my lbgroup').

vServerName Name of the virtual server to bind to the group. Multiple names can be specified.

Example

bind lb group webgrp http_vip To bind multiple vservers to a group use the following command: bind lb group webgrp v To bind vserver v1 to group webgrp1, v2 to webgrp2 and v3 to webgrp3, use the following command: bind lb group webgrp v

set lb group

Configures persistence for the specified load balancing group. The persistence settings are applied to all the members of the group.

Synopsis

set lb group <name>@

Arguments

name Name of the load balancing virtual server group.

persistenceType Type of persistence for the group. Available settings function as follows:

- SOURCEIP - Create persistence sessions based on the client IP.
- COOKIEINSERT - Create persistence sessions based on a cookie in client requests. The cookie is inserted by a Set-Cookie directive from the server, in its first response to a client.
- RULE - Create persistence sessions based on a user defined rule.
- NONE - Disable persistence for the group.

Possible values: SOURCEIP, COOKIEINSERT, RULE, NONE

persistenceBackup Type of backup persistence for the group.

Possible values: SOURCEIP, NONE

backupPersistenceTimeout Time period, in minutes, for which backup persistence is in effect. Default value: 2 Minimum value: 2 Maximum value: 1440

persistMask Persistence mask to apply to source IPv4 addresses when creating source IP based persistence sessions. Default value: 0xFFFFFFFF

cookieName Use this parameter to specify the cookie name for COOKIE peristence type. It specifies the name of cookie with a maximum of 32 characters. If not specified, cookie name is internally generated.

v6persistmasklen Persistence mask to apply to source IPv6 addresses when creating source IP based persistence sessions. Default value: 128 Minimum value: 1 Maximum value: 128

cookieDomain Domain attribute for the HTTP cookie.

timeout Time period for which a persistence session is in effect. Default value: 2 Maximum value: 1440

rule Expression, or name of a named expression, against which traffic is evaluated.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Default value: "None"

useVserverPersistency Use this parameter to enable vserver level persistence on group members. This allows member vservers to have their own persistence, but need to be compatible with other members persistence rules. When this setting is enabled persistence sessions created by any of the members can be shared by other member vservers.

Possible values: ENABLED, DISABLED Default value: DISABLED

masterVserver When USE_VSERVER_PERSISTENCE is enabled, one can use this setting to designate a member vserver as master which is responsible to create the persistence sessions

Example

set lb group webgrp -persistenceType COOKIEINSERT To set the persistence type for multiple groups use the following command: set lb group webgrp -persistenceType COOKIEINSERT

show lb group

Displays the virtual servers bound to the specified group.

Synopsis

show lb group

Arguments

name Name of the load balancing virtual server group.

Output

vServerName Virtual server name.

persistenceType The type of the persistence set for the group.

persistenceBackup The type of the backup persistence set for the group.

backupPersistenceTimeout Time period, in minutes, for which backup persistence is in effect.

persistMask The netmask applied for ipv4 traffic when the persistency type is SOURCEIP.

v6persistmasklen The netmask applied for ipv6 traffic when the persistency type is SOURCEIP.

cookieName Use this parameter to specify the cookie name for COOKIE peristence type. It specifies the name of cookie with a maximum of 32 characters. If not specified, cookie name is internally generated.

cookieDomain Domain attribute for the HTTP cookie.

timeout Time period for which a persistence session is in effect.

rule Rule type.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

stateflag useVserverPersistency Use this parameter to enable vserver level persistence on group members. This allows member vservers to have their own persistence, but need to be compatible with other members persistence rules. When this setting is enabled persistence sessions created by any of the members can be shared by other member vservers.

masterVserver When USE_VSERVER_PERSISTENCE is enabled, one can use this setting to designate a member vserver as master which is responsible to create the persistence sessions

devno count

Example

show lb group webgrp

Related Commands

- add vserver

rm lb group

Removes the lb group

Synopsis

rm lb group <name>@ ...

Arguments

name Name of the lb group to delete.

Example

rm lb group lb_grp1

unset lb group

Use this command to remove lb group settings.Refer to the set lb group command for meanings of the arguments.

Synopsis

unset lb group <name>@

rename lb group

Renames a load balancing virtual server group.

Synopsis

rename lb group <name>@ <newName>@

Arguments

name Existing name of the load balancing virtual server group.

newName New name for the load balancing virtual server group.

Example

rename lb group gv1 gv-new1

add lb group

Adds lb group entity

Synopsis

add lb group <name>@

Arguments

name Name of the load balancing virtual server group.

persistenceType Type of persistence for the group. Available settings function as follows:

- SOURCEIP - Create persistence sessions based on the client IP.

- COOKIEINSERT - Create persistence sessions based on a cookie in client requests. The cookie is inserted by a Set-Cookie directive from the server, in its first response to a client.
- RULE - Create persistence sessions based on a user defined rule.
- NONE - Disable persistence for the group.

Possible values: SOURCEIP, COOKIEINSERT, RULE, NONE

persistenceBackup Type of backup persistence for the group.

Possible values: SOURCEIP, NONE

backupPersistenceTimeout Time period, in minutes, for which backup persistence is in effect. Default value: 2 Minimum value: 2 Maximum value: 1440

persistMask Persistence mask to apply to source IPv4 addresses when creating source IP based persistence sessions. Default value: 0xFFFFFFFF

cookieName Use this parameter to specify the cookie name for COOKIE peristence type. It specifies the name of cookie with a maximum of 32 characters. If not specified, cookie name is internally generated.

v6persistmasklen Persistence mask to apply to source IPv6 addresses when creating source IP based persistence sessions. Default value: 128 Minimum value: 1 Maximum value: 128

cookieDomain Domain attribute for the HTTP cookie.

timeout Time period for which a persistence session is in effect. Default value: 2 Maximum value: 1440

rule Expression, or name of a named expression, against which traffic is evaluated.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Default value: "None"

masterVserver When USE_VSERVER_PERSISTENCE is enabled, one can use this setting to designate a member vserver as master which is responsible to create the persistence sessions

useVserverPersistency Use this parameter to enable vserver level persistence on group members. This allows member vservers to have their own persistence, but need to be compatible with other members persistence rules. When this setting is enabled persistence sessions created by any of the members can be shared by other member vservers.

Possible values: ENABLED, DISABLED Default value: DISABLED

lb-metricTable

The following operations can be performed on "lb-metricTable":

add| unbind| set| rm| bind| show|

add lb metricTable

Creates a metric table for load monitoring.

Synopsis

add lb metricTable <metricTable>

Arguments

metricTable Name for the metric table. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my metrictable" or 'my metrictable').

Example

add metrictable newtable

unbind lb metricTable

Unbinds a metric from a metric table.

Synopsis

unbind lb metricTable <metricTable> <metric>

Arguments

metricTable Name of the metric table.

metric Name of the metric to unbind.

Example

unbind metrictable tablename aliasname

set lb metricTable

Modifies the SNMP OID of a metric in a metric table.

Synopsis

set lb metricTable <metricTable> <metric> <snmpOID>

Arguments

metricTable Name of the metric table.

metric Name of the metric for which to change the SNMP OID.

snmpOID New SNMP OID of the metric.

Example

set metrictable table met1 aliasname oidstr

rm lb metricTable

Removes a metric table.

Synopsis

rm lb metricTable <metricTable>

Arguments

metricTable Name of the metric table.

Example

rm metric table netscaler

bind lb metricTable

Binds a metric to a metric table. You must also specify the SNMP OID of the metric.

Synopsis

bind lb metricTable <metricTable> <metric> <snmpOID>

Arguments

metricTable Name of the metric table.

metric Name of the metric.

snmpOID SNMP OID of the metric.

Example

bind metrictable tablename aliasname 1.2.3.4

show lb metricTable

Displays the parameters of the specified metric table. If no metric table name is specified, a list of all configured metric tables is displayed.

Synopsis

show lb metricTable

Arguments

metricTable Name of the metric table.

Output

metric Metric name of the oid.

snmpOID OID corresponding to the metric

flags flags controlling display

stateflag flags controlling display

metricType Indication if it is a configured or internal

type Adds a temporary or permanent table.

builtin feature The feature to be checked while applying this config

devno count

Example

An example of the show metrictable command output is as follows: Name : ALTEON Type : INTERNAL Name : CISCO-CSS Type : INTERNAL Name : FOUNDRY Type : INTERNAL Name : NETSCALER Type : INTERNAL Name : F5 Type : INTERNAL Name : local Type : INTERNAL

lb-monbindings

The following operations can be performed on "lb-monbindings":

show lb monbindings

Display the services to which this monitor is bound

Synopsis

show lb monbindings <monitorName>

Arguments

monitorName The name of the monitor.

Output

type The type of monitor.

state The state of the monitor.

boundServiceGroupSvrState The state of the servicegroup.

monsvcState The configured state (enable/disable) of Monitor on this service.

monState The configured state (enable/disable) of Monitor on this service.

IPAddress The IPAddress of the service.

port The port of the service.

serviceName The name of the service.

serviceGroupName The name of the service group.

serviceType The type of service

svrState The state of the service

stateflag devno count

lb-monitor

The following operations can be performed on "lb-monitor":

bind| rm| disable| unbind| unset| show| set| add| enable|

bind lb monitor

Binds a monitor to a service or service group. Multiple monitors can be bound to a service or service group.

Synopsis

bind lb monitor <monitorName> [-metric <string> -metricThreshold <positive_integer>] [-certkeyName <string> [-CA]]

Arguments

monitorName Name of the monitor.

metric Name of the metric to be polled by the monitor.

metricThreshold Threshold for the specified metric. A value of zero disables the metric (the metric will not be used in load calculations). Minimum value: 0

metricWeight Weight to assign to the specified metric. A higher number specifies greater weight. Default value: 1 Minimum value: 1 Maximum value: 100

certkeyName The name of the CertKey

CA CA certificate.

crlCheck The state of the CRL check parameter. (Mandatory/Optional)

Possible values: Mandatory, Optional

ocspCheck The state of the OCSP check parameter. (Mandatory/Optional)

Possible values: Mandatory, Optional

Example

bind monitor http_mon http_svc To bind a monitor to multiple services use the following command: bind monitor http_mon http_svc

rm lb monitor

Removes a monitor or a response code for an HTTP monitor. If you do not specify any response codes, the monitor is removed. If you provide any or all of the HTTP response codes that are configured for the monitor, only those specified response codes are removed; the monitor is not removed. Built-in monitors cannot be removed.

Synopsis

rm lb monitor <monitorName> <type> [-respCode <int> ...]

Arguments

monitorName Name of the monitor.

type Type of monitor that you want to create.

Possible values: PING, TCP, HTTP, TCP-ECV, HTTP-ECV, UDP-ECV, DNS, FTP, LDNS-PING, LDNS-TCP, LDNS-DNS, RADIUS, USER, HTTP-INLINE, SIP-UDP, SIP-TCP, LOAD, FTP-EXTENDED, SMTP, SNMP, NNTP, MYSQL, MYSQL-ECV, MSSQL-ECV, ORACLE-ECV, LDAP, POP3, CITRIX-XML-SERVICE, CITRIX-WEB-INTERFACE, DNS-TCP, RTSP, ARP, CITRIX-AG, CITRIX-AAC-LOGINPAGE, CITRIX-AAC-LAS, CITRIX-XD-DDC, ND6, CITRIX-WI-EXTENDED, DIAMETER, RADIUS_ACCOUNTING, STOREFRONT, APPC, SMPP, CITRIX-XNC-ECV, CITRIX-XDM, CITRIX-STA-SERVICE, CITRIX-STA-SERVICE-NHOP, MQTT, HTTP2

respCode Response codes to delete from the response code list configured for the HTTP monitor.

Example

rm monitor http_mon http

disable lb monitor

Disable the monitor for a service. If the monitor name is not specified, all monitors bound to the service are disabled.

Synopsis

disable lb monitor (<serviceName>@ | <serviceGroupName>@)

Arguments

serviceName The name of the service being monitored.

serviceGroupName The name of the service group being monitored.

monitorName Name for the monitor. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my monitor" or 'my monitor').

Example

disable monitor http_svc http_mon To disable a monitor on multiple services use the following command: disable monitor http_svc http_mon

Related Commands

- add service

unbind lb monitor

Unbinds a monitor from a service or service group.

Synopsis

unbind lb monitor <monitorName> [-certkeyName <string>]

Arguments

monitorName Name of the monitor.

metric Name of the metric to be polled by the monitor.

certkeyName The name of the CertKey

CA The rule for use of CRL corresponding to this CA certificate during client authentication. If crlCheck is set to Mandatory, the system will deny all SSL clients if the CRL is missing, expired - NextUpdate date is in the past, or is incomplete with remote CRL refresh enabled. If crlCheck is set to optional, the system will allow SSL clients in the above error cases.However, in any case if the client certificate is revoked in the CRL, the SSL client will be denied access.

Example

unbind monitor http_mon http_svc To unbind a monitor to multiple services use the following command: unbind monitor http_mon http_svc

unset lb monitor

Removes the specified parameter settings from the specified monitor. Attributes for which a default value is available revert to their default values..Refer to the set lb monitor command for meanings of the arguments.

Synopsis

unset lb monitor <monitorName> <type>

Example

set monitor dns_mon dns -ipaddress 10.102.27.230

show lb monitor

Displays the parameters of all the monitors configured on the appliance, or the parameters of the specified monitor.

Synopsis

show lb monitor show lb monitor bindings - alias for 'show lb monbindings'

Arguments

monitorName Name of the monitor.

type Type of monitor that you want to create.

Possible values: PING, TCP, HTTP, TCP-ECV, HTTP-ECV, UDP-ECV, DNS, FTP, LDNS-PING, LDNS-TCP, LDNS-DNS, RADIUS, USER, HTTP-INLINE, SIP-UDP, SIP-TCP, LOAD, FTP-EXTENDED, SMTP, SNMP, NNTP, MYSQL, MYSQL-ECV, MSSQL-ECV, ORACLE-ECV, LDAP, POP3, CITRIX-XML-SERVICE, CITRIX-WEB-INTERFACE, DNS-TCP, RTSP, ARP, CITRIX-AG, CITRIX-AAC-LOGINPAGE, CITRIX-AAC-LAS, CITRIX-XD-DDC, ND6, CITRIX-WI-EXTENDED, DIAMETER, RADIUS_ACCOUNTING, STOREFRONT, APPC, SMPP, CITRIX-XNC-ECV, CITRIX-XDM, CITRIX-STA-SERVICE, CITRIX-STA-SERVICE-NHOP, MQTT, HTTP2

Output

interval The frequency at which the probe is sent to the service.

units monitor interval units

resptimeout The interval for which the system waits before it marks the probe as FAILED.

resptimeoutThresh Response time threshold, specified as a percentage of the Response Time-out parameter. If the response to a monitor probe has not arrived when the threshold is reached, the appliance generates an SNMP trap called monRespTimeoutAboveThresh. After the response time returns to a value below the threshold, the appliance generates a monRespTimeoutBelowThresh SNMP trap. For the traps to be generated, the "MONITOR-RTO-THRESHOLD" alarm must also be enabled.

units monitor response timeout units

retries Maximum number of probes to send to establish the state of a service for which a monitoring probe failed.

failureRetries Number of retries that must fail, out of the number specified for the Retries parameter, for a service to be marked as DOWN. For example, if the Retries parameter is set to 10 and the Failure Retries parameter is set to 6, out of the ten probes sent, at least six probes must fail if the service is to be marked as DOWN. The default value of 0 means that all the retries must fail if the service is to be marked as DOWN.

alertRetries The number of failures after which the system generates a SNMP trap.

successRetries Number of consecutive successful probes required to transition a service's state from DOWN to UP.

downTime The duration in seconds for which the system waits to make the next probe once the service is marked as DOWN.

units Unit of measurement for the Down Time parameter. Cannot be changed after the monitor is created.

destIP The IP address to which the probe is sent.

destPort The TCP/UDP port to which the probe is sent.

state The state of the monitor.

reverse Mark a service as DOWN, instead of UP, when probe criteria are satisfied, and as UP instead of DOWN when probe criteria are not satisfied.

transparent The state of the monitor for transparent devices.

ipTunnel The state of the monitor for tunneled devices.

tos TOS setting.

tosId TOS ID

secure The state of the secure monitoring of services.

action Action to perform when the response to an inline monitor (a monitor of type HTTP-INLINE) indicates that the service is down. A service monitored by an inline monitor is considered DOWN if the response code is not one of the codes that have been specified for the Response Code parameter. Available settings function as follows:

- NONE - Do not take any action. However, the show service command and the show lb monitor command indicate the total number of responses that were checked and the number of consecutive error responses received after the last successful probe.
- LOG - Log the event in NSLOG or SYSLOG.
- DOWN - Mark the service as being down, and then do not direct any traffic to the service until the configured down time has expired. Persistent connections to the service are terminated as soon as the service is marked as DOWN. Also, log the event in NSLOG or SYSLOG.

respCode The response codes.

httpRequest The HTTP request that is sent to the server.

rtspRequest The RTSP request that is sent to the server.

send The string that is sent to the service.

recv The string that is expected from the server to mark the server as UP.

query Domain name to resolve as part of monitoring the DNS service (for example, example.com).

queryType Type of DNS record for which to send monitoring queries. Set to Address for querying A records, AAAA for querying AAAA records, and Zone for querying the SOA record.

userName Username on the RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3/CITRIX-XD-DDC/CITRIX-WI-EXTENDED/CITRIX-XNC-ECV/CITRIX-XDM/MQTT server. This user name is used in the probe.

password Password used in RADIUS/NNTP/FTP/FTP-EXTENDED/MYSQL/POP3/LDAP/CITRIX-XD-DDC/CITRIX-WI-EXTENDED/CITRIX-XNC-ECV/CITRIX-XDM/MQTT server monitoring.

secondaryPassword Secondary password that users might have to provide to log on to the Access Gateway server. Applicable to CITRIX-AG monitors.

logonpointName Logonpoint name used in Citrix AAC login page monitoring.

lasVersion Version number of the Citrix Advanced Access Control Logon Agent. Required by the CITRIX-AAC-LAS monitor.

validateCred Validate the credentials of the Xen Desktop DDC server user. Applicable to monitors of type CITRIX-XD-DDC.

domain Domain in which the XenDesktop Desktop Delivery Controller (DDC) servers or Web Interface servers are present. Required by CITRIX-XD-DDC and CITRIX-WI-EXTENDED monitors for logging on to the DDC servers and Web Interface servers, respectively.

radKey Authentication key (shared secret text string) for RADIUS clients and servers to exchange. Applicable to monitors of type RADIUS and RADIUS_ACCOUNTING.

radNASid NAS-Identifier to send in the Access-Request packet. Applicable to monitors of type RADIUS.

radNASip Network Access Server (NAS) IP address to use as the source IP address when monitoring a RADIUS server. Applicable to monitors of type RADIUS and RADIUS_ACCOUNTING.

radAccountType Account Type to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING.

radFramedIP Source ip with which the packet will go out . Applicable to monitors of type RADIUS_ACCOUNTING.

radAPN Called Station Id to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING.

radMSISDN Calling Stations Id to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING.

radAccountSession Account Session ID to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING.

LRTM Calculate the least response times for bound services. If this parameter is not enabled, the appliance does not learn the response times of the bound services. Also used for LRTM load balancing.

lrtmConf State of LRTM configuration on the monitor.

lrtmConfStr State of LRTM configuration on the monitor as STRING.

deviation Deviation from the learnt response time for Dynamic Response Time monitoring.

units Unit of measurement for the Deviation parameter. Cannot be changed after the monitor is created.

dynamicResponseTimeout Response timeout of the DRTM enabled monitor , calculated dynamically based on the history and current response time.

dynamicInterval Interval between monitoring probes for DRTM enabled monitor , calculated dynamically based monitor response time.

scriptName Path and name of the script to execute. The script must be available on the Citrix ADC, in the /nsconfig/monitors/ directory.

scriptArgs String of arguments for the script. The string is copied verbatim into the request.

secureArgs List of arguments for the script which should be secure

dispatcherIP IP address of the dispatcher to which to send the probe.

dispatcherPort Port number on which the dispatcher listens for the monitoring probe.

sipURI SIP URI string to send to the service (for example, sip:sip.test). Applicable only to monitors of type SIP-UDP.

sipMethod Specifies SIP method to be used for the query

maxForwards Maximum number of hops a sip monitor packet can go.

sipregURI Specifies SIP user to be registered

customHeaders The string that is sent to the service. Applicable to HTTP ,HTTP-ECV and RTSP monitor types.

IPAddress Set of IP addresses expected in the monitoring response from the DNS server, if the record type is A or AAAA. Applicable to DNS monitors.

group Name of a newsgroup available on the NNTP service that is to be monitored. The appliance periodically generates an NNTP query for the name of the newsgroup and evaluates the response. If the newsgroup is found on the server, the service is marked as UP. If the newsgroup does not exist or if the search fails, the service is marked as DOWN. Applicable to NNTP monitors.

fileName Name of a file on the FTP server. The appliance monitors the FTP service by periodically checking the existence of the file on the server. Applicable to FTP-EXTENDED monitors.

baseDN The base distinguished name of the LDAP service, from where the LDAP server can begin the search for the attributes in the monitoring query. Required for LDAP service monitoring.

bindDN The distinguished name with which an LDAP monitor can perform the Bind operation on the LDAP server. Optional. Applicable to LDAP monitors.

filter Filter criteria for the LDAP query. Optional.

attribute Attribute to evaluate when the LDAP server responds to the query. Success or failure of the monitoring probe depends on whether the attribute exists in the response. Optional.

database Name of the database to connect to during authentication.

oracleSid Name of the service identifier that is used to connect to the Oracle database during authentication.

sqlQuery SQL query for a MYSQL-ECV or MSSQL-ECV monitor. Sent to the database server after the server authenticates the connection.

evalRule Expression that evaluates the database server's response to a MYSQL-ECV or MSSQL-ECV monitoring query. Must produce a Boolean result. The result determines the state of the server. If the expression returns TRUE, the probe succeeds. For example, if you want the appliance to evaluate the error message to determine the state of the server, use the rule MYSQL.RES.ROW(10) .TEXT_ELEM(2).EQ("MySQL").

snmpOID SNMP OID for SNMP monitors.

snmpCommunity Community name for SNMP monitors.

snmpThreshold Threshold for SNMP monitors.

snmpVersion SNMP version to be used for SNMP monitoring.

metric Metric name in the metric table, whose setting is changed

metricTable Metric table, whose setting is changed

multimetrictable Metric table to which to bind metrics, to be used only for output purposes.

metricThreshold Threshold to be used for that metric.

metricWeight The weight for the specified service metric with respect to others.

stateflag Flags controlling the display.

flags Used by build-in monitors.

application Name of the application used to determine the state of the service. Applicable to monitors of type CITRIX-XML-SERVICE.

sitePath URL of the logon page. For monitors of type CITRIX-WEB-INTERFACE, to monitor a dynamic page under the site path, terminate the site path with a slash (/). Applicable to CITRIX-WEB-INTERFACE, CITRIX-WI-EXTENDED and CITRIX-XDM monitors.

storename Store Name. For monitors of type STOREFRONT, STORENAME is an optional argument defining storefront service store name. Applicable to STOREFRONT monitors.

storefrontacctservice Enable/Disable probing for Account Service. Applicable only to Store Front monitors. For multi-tenancy configuration users my skip account service

storefrontcheckbackendservices This option will enable monitoring of services running on storefront server. Storefront services are monitored by probing to a Windows service that runs on the Storefront server and exposes details of which storefront services are running.

hostName Hostname in the FQDN format (Example: porche.cars.org). Applicable to STOREFRONT monitors.

units Giving the unit of the metric

netProfile Name of the network profile.

mssqlProtocolVersion Version of MSSQL server that is to be monitored.

originHost Origin-Host value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

originRealm Origin-Realm value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

hostIPAddress Host-IP-Address value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. If Host-IP-Address is not specified, the appliance inserts the mapped IP (MIP) address or subnet IP (SNIP) address from which the CER request (the monitoring probe) is sent.

vendorId Vendor-Id value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

productName Product-Name value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

firmwareRevision Firmware-Revision value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

authApplicationId List of Auth-Application-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring CER message.

acctApplicationId List of Acct-Application-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring message.

inbandSecurityId Inband-Security-Id for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

supportedVendorIds List of Supported-Vendor-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum eight of these AVPs are supported in a monitoring message.

vendorSpecificVendorId Vendor-Id to use in the Vendor-Specific-Application-Id grouped attribute-value pair (AVP) in the monitoring CER message. To specify Auth-Application-Id or Acct-Application-Id in Vendor-Specific-Application-Id, use vendorSpecificAuthApplicationIds or vendorSpecificAcctApplicationIds, respectively. Only one Vendor-Id is supported for all the Vendor-Specific-Application-Id AVPs in a CER monitoring message.

vendorSpecificAuthApplicationIds List of Vendor-Specific-Auth-Application-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring message. The specified value is combined with the value of vendorSpecificVendorId to obtain the Vendor-Specific-Application-Id AVP in the CER monitoring message.

vendorSpecificAcctApplicationIds List of Vendor-Specific-Acct-Application-Id attribute value pairs (AVPs) to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring message. The specified value is combined with the value of vendorSpecificVendorId to obtain the Vendor-Specific-Application-Id AVP in the CER monitoring message.

serviceName state weight serviceGroupName weight kcdAccount KCD Account used by MSSQL monitor

storedb Store the database list populated with the responses to monitor probes. Used in database specific load balancing if MSSQL-ECV/MYSQL-ECV monitor is configured.

trofscode Code expected when the server is under maintenance

trofsstring String expected from the server for the service to be marked as trofs. Applicable to HTTP-ECV/TCP-ECV monitors.

sslProfile SSL Profile associated with the monitor

certkeyName The name of the certificate bound to the monitor.

CA The rule for use of CRL corresponding to this CA certificate during client authentication. If crlCheck is set to Mandatory, the system will deny all SSL clients if the CRL is missing, expired - NextUpdate date is in the past, or is incomplete with remote CRL refresh enabled. If crlCheck is set to optional, the system will allow SSL clients in the above error cases.However, in any case if the client certificate is revoked in the CRL, the SSL client will be denied access.

crlCheck The state of the CRL check parameter. (Mandatory/Optional)

ocspCheck The state of the OCSP check parameter. (Mandatory/Optional)

mqttClientIdentifier Client id to be used in Connect command

mqttVersion Version of MQTT protocol used in connect message, default is version 3.1.1

grpcHealthCheck Option to enable or disable gRPC health check service.

grpcStatusCode gRPC status codes for which to mark the service as UP. The default value is 12(health check unimplemented). If the gRPC status code 0 is received from the backend this configuration is ignored.

grpcServiceName Option to specify gRPC service name on which gRPC health check need to be performed

devno count

Example

An example of the show monitor command output is as follows: 8 configured monitors:

1. Name.....: ping Type.....: PING State....ENABLED
2. Name.....: tcp Type.....: TCP State....ENABLED
3. Name.....: http Type.....: HTTP State....ENABLED

4. Name.....: tcp-ecv Type.....: TCP-ECV State....ENABLED
5. Name.....: http-ecv Type.....: HTTP-ECV State....ENABLED
6. Name.....: udp-ecv Type.....: UDP-ECV State....ENABLED
7. Name.....: dns Type.....: DNS State....ENABLED
8. Name.....: ftp Type.....: FTP State....ENABLED

set lb monitor

Modifies the specified parameters of a monitor.

Synopsis

set lb monitor <monitorName> <type> [-respCode <int> ...] {-password } {-secondaryPassword } {-radKey } [-deviation <positive_integer>] [-interval <integer>] [-resptimeout <integer>] [-downTime <integer>] [-metric <string>] [-vendorSpecificVendorId <positive_integer>]

Arguments

monitorName Name of the monitor.

type Type of monitor that you want to create.

Possible values: PING, TCP, HTTP, TCP-ECV, HTTP-ECV, UDP-ECV, DNS, FTP, LDNS-PING, LDNS-TCP, LDNS-DNS, RADIUS, USER, HTTP-INLINE, SIP-UDP, SIP-TCP, LOAD, FTP-EXTENDED, SMTP, SNMP, NNTP, MYSQL, MYSQL-ECV, MSSQL-ECV, ORACLE-ECV, LDAP, POP3, CITRIX-XML-SERVICE, CITRIX-WEB-INTERFACE, DNS-TCP, RTSP, ARP, CITRIX-AG, CITRIX-AAC-LOGINPAGE, CITRIX-AAC-LAS, CITRIX-XD-DDC, ND6, CITRIX-WI-EXTENDED, DIAMETER, RADIUS_ACCOUNTING, STOREFRONT, APPC, SMPP, CITRIX-XNC-ECV, CITRIX-XDM, CITRIX-STA-SERVICE, CITRIX-STA-SERVICE-NHOP, MQTT, HTTP2

action Action to perform when the response to an inline monitor (a monitor of type HTTP-INLINE) indicates that the service is down. A service monitored by an inline monitor is considered DOWN if the response code is not one of the codes that have been specified for the Response Code parameter. Available settings function as follows:

- NONE - Do not take any action. However, the show service command and the show lb monitor command indicate the total number of responses that were checked and the number of consecutive error responses received after the last successful probe.
- LOG - Log the event in NSLOG or SYSLOG.

- DOWN - Mark the service as being down, and then do not direct any traffic to the service until the configured down time has expired. Persistent connections to the service are terminated as soon as the service is marked as DOWN. Also, log the event in NSLOG or SYSLOG.

Possible values: NONE, LOG, DOWN Default value: DOWN

respCode Response codes for which to mark the service as UP. For any other response code, the action performed depends on the monitor type. HTTP monitors and RADIUS monitors mark the service as DOWN, while HTTP-INLINE monitors perform the action indicated by the Action parameter.

httpRequest HTTP request to send to the server (for example, "HEAD /file.html").

rtspRequest RTSP request to send to the server (for example, "OPTIONS *").

customHeaders Custom header string to include in the monitoring probes.

maxForwards Maximum number of hops that the SIP request used for monitoring can traverse to reach the server. Applicable only to monitors of type SIP-UDP. Default value: 1 Minimum value: 0 Maximum value: 255

sipMethod SIP method to use for the query. Applicable only to monitors of type SIP-UDP.

Possible values: OPTIONS, INVITE, REGISTER

sipregURI SIP user to be registered. Applicable only if the monitor is of type SIP-UDP and the SIP Method parameter is set to REGISTER.

sipURI SIP URI string to send to the service (for example, sip:sip.test). Applicable only to monitors of type SIP-UDP.

send String to send to the service. Applicable to TCP-ECV, HTTP-ECV, and UDP-ECV monitors.

recv String expected from the server for the service to be marked as UP. Applicable to TCP-ECV, HTTP-ECV, and UDP-ECV monitors.

query Domain name to resolve as part of monitoring the DNS service (for example, example.com).

queryType Type of DNS record for which to send monitoring queries. Set to Address for querying A records, AAAA for querying AAAA records, and Zone for querying the SOA record.

Possible values: Address, Zone, AAAA

userName User name with which to probe the RADIUS, NNTP, FTP, FTP-EXTENDED, MYSQL, MSSQL, POP3, CITRIX-AG, CITRIX-XD-DDC, CITRIX-WI-EXTENDED, CITRIX-XNC or CITRIX-XDM server.

password Password that is required for logging on to the RADIUS, NNTP, FTP, FTP-EXTENDED, MYSQL, MSSQL, POP3, CITRIX-AG, CITRIX-XD-DDC, CITRIX-WI-EXTENDED, CITRIX-XNC-ECV or CITRIX-XDM server. Used in conjunction with the user name specified for the User Name parameter.

secondaryPassword Secondary password that users might have to provide to log on to the Access Gateway server. Applicable to CITRIX-AG monitors.

logonpointName Name of the logon point that is configured for the Citrix Access Gateway Advanced Access Control software. Required if you want to monitor the associated login page or Logon Agent. Applicable to CITRIX-AAC-LAS and CITRIX-AAC-LOGINPAGE monitors.

lasVersion Version number of the Citrix Advanced Access Control Logon Agent. Required by the CITRIX-AAC-LAS monitor.

radKey Authentication key (shared secret text string) for RADIUS clients and servers to exchange. Applicable to monitors of type RADIUS and RADIUS_ACCOUNTING.

radNASid NAS-Identifier to send in the Access-Request packet. Applicable to monitors of type RADIUS.

radNASip Network Access Server (NAS) IP address to use as the source IP address when monitoring a RADIUS server. Applicable to monitors of type RADIUS and RADIUS_ACCOUNTING.

radAccountType Account Type to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING. Default value: 1 Minimum value: 0 Maximum value: 15

radFramedIP Source ip with which the packet will go out . Applicable to monitors of type RADIUS_ACCOUNTING.

radAPN Called Station Id to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING.

radMSISDN Calling Stations Id to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING.

radAccountSession Account Session ID to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING.

LRTM Calculate the least response times for bound services. If this parameter is not enabled, the appliance does not learn the response times of the bound services. Also used for LRTM load balancing.

Possible values: ENABLED, DISABLED

deviation Time value added to the learned average response time in dynamic response time monitoring (DRTM). When a deviation is specified, the appliance learns the average response time of bound services and adds the deviation to the average. The final value is then continually adjusted to accommodate response time variations over time. Specified in milliseconds, seconds, or minutes. Minimum value: 0 Maximum value: 20939

units Unit of measurement for the Deviation parameter. Cannot be changed after the monitor is created.

Possible values: SEC, MSEC, MIN Default value: SEC

scriptName Path and name of the script to execute. The script must be available on the Citrix ADC, in the /nsconfig/monitors/ directory.

scriptArgs String of arguments for the script. The string is copied verbatim into the request.

secureArgs List of arguments for the script which should be secure

validateCred Validate the credentials of the Xen Desktop DDC server user. Applicable to monitors of type CITRIX-XD-DDC.

Possible values: YES, NO Default value: NO

domain Domain in which the XenDesktop Desktop Delivery Controller (DDC) servers or Web Interface servers are present. Required by CITRIX-XD-DDC and CITRIX-WI-EXTENDED monitors for logging on to the DDC servers and Web Interface servers, respectively.

dispatcherIP IP address of the dispatcher to which to send the probe.

dispatcherPort Port number on which the dispatcher listens for the monitoring probe.

interval Time interval between two successive probes. Must be greater than the value of Response Time-out. Default value: 5 Minimum value: 1 Maximum value: 20940

units monitor interval units

Possible values: SEC, MSEC, MIN Default value: SEC

resptimeout Amount of time for which the appliance must wait before it marks a probe as FAILED. Must be less than the value specified for the Interval parameter.

Note: For UDP-ECV monitors for which a receive string is not configured, response timeout does not apply. For UDP-ECV monitors with no receive string, probe failure is indicated by an ICMP port unreachable error received from the service. Default value: 2 Minimum value: 1 Maximum value: 20939

units monitor response timeout units

Possible values: SEC, MSEC, MIN Default value: SEC

resptimeoutThresh Response time threshold, specified as a percentage of the Response Time-out parameter. If the response to a monitor probe has not arrived when the threshold is reached, the appliance generates an SNMP trap called monRespTimeoutAboveThresh. After the response time returns to a value below the threshold, the appliance generates a monRespTimeoutBelowThresh SNMP trap. For the traps to be generated, the "MONITOR-RTO-THRESHOLD" alarm must also be enabled. Minimum value: 0 Maximum value: 100

retries Maximum number of probes to send to establish the state of a service for which a monitoring probe failed. Default value: 3 Minimum value: 1 Maximum value: 127

failureRetries Number of retries that must fail, out of the number specified for the Retries parameter, for a service to be marked as DOWN. For example, if the Retries parameter is set to 10 and the Failure Retries parameter is set to 6, out of the ten probes sent, at least six probes must fail if the service is to be marked as DOWN. The default value of 0 means that all the retries must fail if the service is to be marked as DOWN. Maximum value: 32

alertRetries Number of consecutive probe failures after which the appliance generates an SNMP trap called monProbeFailed. Maximum value: 32

successRetries Number of consecutive successful probes required to transition a service's state from DOWN to UP. Default value: 1 Minimum value: 1 Maximum value: 32

downTime Time duration for which to wait before probing a service that has been marked as DOWN. Expressed in milliseconds, seconds, or minutes. Default value: 30 Minimum value: 1 Maximum value: 20939

units Unit of measurement for the Down Time parameter. Cannot be changed after the monitor is created.

Possible values: SEC, MSEC, MIN Default value: SEC

destIP IP address of the service to which to send probes. If the parameter is set to 0, the IP address of the server to which the monitor is bound is considered the destination IP address.

destPort TCP or UDP port to which to send the probe. If the parameter is set to 0, the port number of the service to which the monitor is bound is considered the destination port. For a monitor of type USER, however, the destination port is the port number that is included in the HTTP request sent to the dispatcher. Does not apply to monitors of type PING.

state State of the monitor. The DISABLED setting disables not only the monitor being configured, but all monitors of the same type, until the parameter is set to ENABLED. If the monitor is bound to a service, the state of the monitor is not taken into account when the state of the service is determined.

Possible values: ENABLED, DISABLED Default value: ENABLED

reverse Mark a service as DOWN, instead of UP, when probe criteria are satisfied, and as UP instead of DOWN when probe criteria are not satisfied.

Possible values: YES, NO Default value: NO

transparent The monitor is bound to a transparent device such as a firewall or router. The state of a transparent device depends on the responsiveness of the services behind it. If a transparent device is being monitored, a destination IP address must be specified. The probe is sent to the specified IP address by using the MAC address of the transparent device.

Possible values: YES, NO Default value: NO

ipTunnel Send the monitoring probe to the service through an IP tunnel. A destination IP address must be specified.

Possible values: YES, NO Default value: NO

tos Probe the service by encoding the destination IP address in the IP TOS (6) bits.

Possible values: YES, NO

tosId The TOS ID of the specified destination IP. Applicable only when the TOS parameter is set. Minimum value: 1 Maximum value: 63

secure Use a secure SSL connection when monitoring a service. Applicable only to TCP based monitors. The secure option cannot be used with a CITRIX-AG monitor, because a CITRIX-AG monitor uses a secure connection by default.

Possible values: YES, NO Default value: NO

IPAddress Set of IP addresses expected in the monitoring response from the DNS server, if the record type is A or AAAA. Applicable to DNS monitors.

group Name of a newsgroup available on the NNTP service that is to be monitored. The appliance periodically generates an NNTP query for the name of the newsgroup and evaluates the response. If the newsgroup is found on the server, the service is marked as UP. If the newsgroup does not exist or if the search fails, the service is marked as DOWN. Applicable to NNTP monitors.

fileName Name of a file on the FTP server. The appliance monitors the FTP service by periodically checking the existence of the file on the server. Applicable to FTP-EXTENDED monitors.

baseDN The base distinguished name of the LDAP service, from where the LDAP server can begin the search for the attributes in the monitoring query. Required for LDAP service monitoring.

bindDN The distinguished name with which an LDAP monitor can perform the Bind operation on the LDAP server. Optional. Applicable to LDAP monitors.

filter Filter criteria for the LDAP query. Optional.

attribute Attribute to evaluate when the LDAP server responds to the query. Success or failure of the monitoring probe depends on whether the attribute exists in the response. Optional.

database Name of the database to connect to during authentication.

oracleSid Name of the service identifier that is used to connect to the Oracle database during authentication.

sqlQuery SQL query for a MYSQL-ECV or MSSQL-ECV monitor. Sent to the database server after the server authenticates the connection.

evalRule Expression that evaluates the database server's response to a MYSQL-ECV or MSSQL-ECV monitoring query. Must produce a Boolean result. The result determines the state of the server. If the expression returns TRUE, the probe succeeds. For example, if you want the appliance to evaluate the error message to determine the state of the server, use the rule MYSQL.RES.ROW(10) .TEXT_ELEM(2).EQ("MySQL").

snmpOID SNMP OID for SNMP monitors.

snmpCommunity Community name for SNMP monitors.

snmpThreshold Threshold for SNMP monitors.

snmpVersion SNMP version to be used for SNMP monitors.

Possible values: V1, V2

metricTable Metric table to which to bind metrics.

metric Metric name in the metric table, whose setting is changed. A value zero disables the metric and it will not be used for load calculation

metricThreshold Threshold to be used for that metric. Minimum value: 0

metricWeight The weight for the specified service metric with respect to others. Minimum value: 1 Maximum value: 100

application Name of the application used to determine the state of the service. Applicable to monitors of type CITRIX-XML-SERVICE.

sitePath URL of the logon page. For monitors of type CITRIX-WEB-INTERFACE, to monitor a dynamic page under the site path, terminate the site path with a slash (/). Applicable to CITRIX-WEB-INTERFACE, CITRIX-WI-EXTENDED and CITRIX-XDM monitors.

storename Store Name. For monitors of type STOREFRONT, STORENAME is an optional argument defining storefront service store name. Applicable to STOREFRONT monitors.

storefrontacctservice Enable/Disable probing for Account Service. Applicable only to Store Front monitors. For multi-tenancy configuration users my skip account service

Possible values: YES, NO Default value: YES

storefrontcheckbackendservices This option will enable monitoring of services running on storefront server. Storefront services are monitored by probing to a Windows service that runs on the Storefront server and exposes details of which storefront services are running.

Possible values: YES, NO Default value: NO

netProfile Name of the network profile.

mssqlProtocolVersion Version of MSSQL server that is to be monitored.

Possible values: 70, 2000, 2000SP1, 2005, 2008, 2008R2, 2012, 2014 Default value: 70

originHost Origin-Host value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

originRealm Origin-Realm value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

hostIPAddress Host-IP-Address value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. If Host-IP-Address is not specified, the appliance inserts the mapped IP (MIP) address or subnet IP (SNIP) address from which the CER request (the monitoring probe) is sent.

vendorId Vendor-Id value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. Minimum value: 0

productName Product-Name value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

firmwareRevision Firmware-Revision value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. Minimum value: 0

authApplicationId List of Auth-Application-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring CER message. Minimum value: 0 Maximum value: 4294967295

acctApplicationId List of Acct-Application-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring message. Minimum value: 0 Maximum value: 4294967295

inbandSecurityId Inband-Security-Id for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

Possible values: NO_INBAND_SECURITY, TLS

supportedVendorIds List of Supported-Vendor-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum eight of these AVPs are supported in a monitoring message. Minimum value: 1 Maximum value: 4294967295

vendorSpecificVendorId Vendor-Id to use in the Vendor-Specific-Application-Id grouped attribute-value pair (AVP) in the monitoring CER message. To specify Auth-Application-Id or Acct-Application-Id in Vendor-Specific-Application-Id, use vendorSpecificAuthApplicationIds or

vendorSpecificAcctApplicationIds, respectively. Only one Vendor-Id is supported for all the Vendor-Specific-Application-Id AVPs in a CER monitoring message. Minimum value: 1

vendorSpecificAuthApplicationIds List of Vendor-Specific-Auth-Application-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring message. The specified value is combined with the value of vendorSpecificVendorId to obtain the Vendor-Specific-Application-Id AVP in the CER monitoring message. Minimum value: 0 Maximum value: 4294967295

vendorSpecificAcctApplicationIds List of Vendor-Specific-Acct-Application-Id attribute value pairs (AVPs) to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring message. The specified value is combined with the value of vendorSpecificVendorId to obtain the Vendor-Specific-Application-Id AVP in the CER monitoring message. Minimum value: 0 Maximum value: 4294967295

kcdAccount KCD Account used by MSSQL monitor

storedb Store the database list populated with the responses to monitor probes. Used in database specific load balancing if MSSQL-ECV/MYSQL-ECV monitor is configured.

Possible values: ENABLED, DISABLED Default value: DISABLED

trofscode Code expected when the server is under maintenance Minimum value: 0

trofsstring String expected from the server for the service to be marked as trofs. Applicable to HTTP-ECV/TCP-ECV monitors.

sslProfile SSL Profile associated with the monitor

mqttClientIdentifier Client id to be used in Connect command

mqttVersion Version of MQTT protocol used in connect message, default is version 3.1.1 Default value: 4 Minimum value: 3

grpcHealthCheck Option to enable or disable gRPC health check service.

Possible values: YES, NO Default value: NO

grpcStatusCode gRPC status codes for which to mark the service as UP. The default value is 12(health check unimplemented). If the gRPC status code 0 is received from the backend this configuration is ignored. Minimum value: 0

grpcServiceName Option to specify gRPC service name on which gRPC health check need to be performed

Example

set monitor http_mon http -respcode 100

add lb monitor

Creates a monitor that you can bind to load balancing services. The monitor periodically sends probes to those services to test their availability.

Synopsis

add lb monitor <monitorName> <type> [-respCode <int> ...] {-password } {-secondaryPassword } {-radKey } [-deviation <positive_integer>] [-interval <integer>] [-resptimeout <integer>] [-downTime <integer>] [-vendorSpecificVendorId <positive_integer>]

Arguments

monitorName Name for the monitor. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my monitor" or 'my monitor').

type Type of monitor that you want to create.

Possible values: PING, TCP, HTTP, TCP-ECV, HTTP-ECV, UDP-ECV, DNS, FTP, LDNS-PING, LDNS-TCP, LDNS-DNS, RADIUS, USER, HTTP-INLINE, SIP-UDP, SIP-TCP, LOAD, FTP-EXTENDED, SMTP, SNMP, NNTP, MYSQL, MYSQL-ECV, MSSQL-ECV, ORACLE-ECV, LDAP, POP3, CITRIX-XML-SERVICE, CITRIX-WEB-INTERFACE, DNS-TCP, RTSP, ARP, CITRIX-AG, CITRIX-AAC-LOGINPAGE, CITRIX-AAC-LAS, CITRIX-XD-DDC, ND6, CITRIX-WI-EXTENDED, DIAMETER, RADIUS_ACCOUNTING, STOREFRONT, APPC, SMPP, CITRIX-XNC-ECV, CITRIX-XDM, CITRIX-STA-SERVICE, CITRIX-STA-SERVICE-NHOP, MQTT, HTTP2

action Action to perform when the response to an inline monitor (a monitor of type HTTP-INLINE) indicates that the service is down. A service monitored by an inline monitor is considered DOWN if the response code is not one of the codes that have been specified for the Response Code parameter. Available settings function as follows:

- NONE - Do not take any action. However, the show service command and the show lb monitor command indicate the total number of responses that were checked and the number of consecutive error responses received after the last successful probe.
- LOG - Log the event in NSLOG or SYSLOG.
- DOWN - Mark the service as being down, and then do not direct any traffic to the service until the configured down time has expired. Persistent connections to the service are terminated as soon as the service is marked as DOWN. Also, log the event in NSLOG or SYSLOG.

Possible values: NONE, LOG, DOWN Default value: DOWN

respCode Response codes for which to mark the service as UP. For any other response code, the action performed depends on the monitor type. HTTP monitors and RADIUS monitors mark the service as DOWN, while HTTP-INLINE monitors perform the action indicated by the Action parameter.

httpRequest HTTP request to send to the server (for example, "HEAD /file.html").

rtspRequest RTSP request to send to the server (for example, "OPTIONS *").

customHeaders Custom header string to include in the monitoring probes.

maxForwards Maximum number of hops that the SIP request used for monitoring can traverse to reach the server. Applicable only to monitors of type SIP-UDP. Default value: 1 Minimum value: 0 Maximum value: 255

sipMethod SIP method to use for the query. Applicable only to monitors of type SIP-UDP.

Possible values: OPTIONS, INVITE, REGISTER

sipURI SIP URI string to send to the service (for example, sip:sip.test). Applicable only to monitors of type SIP-UDP.

sipregURI SIP user to be registered. Applicable only if the monitor is of type SIP-UDP and the SIP Method parameter is set to REGISTER.

send String to send to the service. Applicable to TCP-ECV, HTTP-ECV, and UDP-ECV monitors.

recv String expected from the server for the service to be marked as UP. Applicable to TCP-ECV, HTTP-ECV, and UDP-ECV monitors.

query Domain name to resolve as part of monitoring the DNS service (for example, example.com).

queryType Type of DNS record for which to send monitoring queries. Set to Address for querying A records, AAAA for querying AAAA records, and Zone for querying the SOA record.

Possible values: Address, Zone, AAAA

scriptName Path and name of the script to execute. The script must be available on the Citrix ADC, in the /nsconfig/monitors/ directory.

scriptArgs String of arguments for the script. The string is copied verbatim into the request.

secureArgs List of arguments for the script which should be secure

dispatcherIP IP address of the dispatcher to which to send the probe.

dispatcherPort Port number on which the dispatcher listens for the monitoring probe.

userName User name with which to probe the RADIUS, NNTP, FTP, FTP-EXTENDED, MYSQL, MSSQL, POP3, CITRIX-AG, CITRIX-XD-DDC, CITRIX-WI-EXTENDED, CITRIX-XNC or CITRIX-XDM server.

password Password that is required for logging on to the RADIUS, NNTP, FTP, FTP-EXTENDED, MYSQL, MSSQL, POP3, CITRIX-AG, CITRIX-XD-DDC, CITRIX-WI-EXTENDED, CITRIX-XNC-ECV or CITRIX-XDM server. Used in conjunction with the user name specified for the User Name parameter.

secondaryPassword Secondary password that users might have to provide to log on to the Access Gateway server. Applicable to CITRIX-AG monitors.

logonpointName Name of the logon point that is configured for the Citrix Access Gateway Advanced Access Control software. Required if you want to monitor the associated login page or Logon Agent. Applicable to CITRIX-AAC-LAS and CITRIX-AAC-LOGINPAGE monitors.

lasVersion Version number of the Citrix Advanced Access Control Logon Agent. Required by the CITRIX-AAC-LAS monitor.

radKey Authentication key (shared secret text string) for RADIUS clients and servers to exchange. Applicable to monitors of type RADIUS and RADIUS_ACCOUNTING.

radNASid NAS-Identifier to send in the Access-Request packet. Applicable to monitors of type RADIUS.

radNASip Network Access Server (NAS) IP address to use as the source IP address when monitoring a RADIUS server. Applicable to monitors of type RADIUS and RADIUS_ACCOUNTING.

radAccountType Account Type to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING. Default value: 1 Minimum value: 0 Maximum value: 15

radFramedIP Source ip with which the packet will go out . Applicable to monitors of type RADIUS_ACCOUNTING.

radAPN Called Station Id to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING.

radMSISDN Calling Stations Id to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING.

radAccountSession Account Session ID to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING.

LRTM Calculate the least response times for bound services. If this parameter is not enabled, the appliance does not learn the response times of the bound services. Also used for LRTM load balancing.

Possible values: ENABLED, DISABLED

deviation Time value added to the learned average response time in dynamic response time monitoring (DRTM). When a deviation is specified, the appliance learns the average response time of bound services and adds the deviation to the average. The final value is then continually adjusted to accommodate response time variations over time. Specified in milliseconds, seconds, or minutes. Minimum value: 0 Maximum value: 20939

units Unit of measurement for the Deviation parameter. Cannot be changed after the monitor is created.

Possible values: SEC, MSEC, MIN Default value: SEC

interval Time interval between two successive probes. Must be greater than the value of Response Time-out. Default value: 5 Minimum value: 1 Maximum value: 20940

units monitor interval units

Possible values: SEC, MSEC, MIN Default value: SEC

resptimeout Amount of time for which the appliance must wait before it marks a probe as FAILED. Must be less than the value specified for the Interval parameter.

Note: For UDP-ECV monitors for which a receive string is not configured, response timeout does not apply. For UDP-ECV monitors with no receive string, probe failure is indicated by an ICMP port unreachable error received from the service. Default value: 2 Minimum value: 1 Maximum value: 20939

units monitor response timeout units

Possible values: SEC, MSEC, MIN Default value: SEC

resptimeoutThresh Response time threshold, specified as a percentage of the Response Time-out parameter. If the response to a monitor probe has not arrived when the threshold is reached, the appliance generates an SNMP trap called monRespTimeoutAboveThresh. After the response time returns to a value below the threshold, the appliance generates a monRespTimeoutBelowThresh SNMP trap. For the traps to be generated, the "MONITOR-RTO-THRESHOLD" alarm must also be enabled. Minimum value: 0 Maximum value: 100

retries Maximum number of probes to send to establish the state of a service for which a monitoring probe failed. Default value: 3 Minimum value: 1 Maximum value: 127

failureRetries Number of retries that must fail, out of the number specified for the Retries parameter, for a service to be marked as DOWN. For example, if the Retries parameter is set to 10 and the Failure Retries parameter is set to 6, out of the ten probes sent, at least six probes must fail if the service is to be marked as DOWN. The default value of 0 means that all the retries must fail if the service is to be marked as DOWN. Maximum value: 32

alertRetries Number of consecutive probe failures after which the appliance generates an SNMP trap called monProbeFailed. Maximum value: 32

successRetries Number of consecutive successful probes required to transition a service's state from DOWN to UP. Default value: 1 Minimum value: 1 Maximum value: 32

downTime Time duration for which to wait before probing a service that has been marked as DOWN. Expressed in milliseconds, seconds, or minutes. Default value: 30 Minimum value: 1 Maximum value: 20939

units Unit of measurement for the Down Time parameter. Cannot be changed after the monitor is created.

Possible values: SEC, MSEC, MIN Default value: SEC

destIP IP address of the service to which to send probes. If the parameter is set to 0, the IP address of the server to which the monitor is bound is considered the destination IP address.

destPort TCP or UDP port to which to send the probe. If the parameter is set to 0, the port number of the service to which the monitor is bound is considered the destination port. For a monitor of type USER, however, the destination port is the port number that is included in the HTTP request sent to the dispatcher. Does not apply to monitors of type PING.

state State of the monitor. The DISABLED setting disables not only the monitor being configured, but all monitors of the same type, until the parameter is set to ENABLED. If the monitor is bound to a service, the state of the monitor is not taken into account when the state of the service is determined.

Possible values: ENABLED, DISABLED Default value: ENABLED

reverse Mark a service as DOWN, instead of UP, when probe criteria are satisfied, and as UP instead of DOWN when probe criteria are not satisfied.

Possible values: YES, NO Default value: NO

transparent The monitor is bound to a transparent device such as a firewall or router. The state of a transparent device depends on the responsiveness of the services behind it. If a transparent device is being monitored, a destination IP address must be specified. The probe is sent to the specified IP address by using the MAC address of the transparent device.

Possible values: YES, NO Default value: NO

ipTunnel Send the monitoring probe to the service through an IP tunnel. A destination IP address must be specified.

Possible values: YES, NO Default value: NO

tos Probe the service by encoding the destination IP address in the IP TOS (6) bits.

Possible values: YES, NO

tosId The TOS ID of the specified destination IP. Applicable only when the TOS parameter is set. Minimum value: 1 Maximum value: 63

secure Use a secure SSL connection when monitoring a service. Applicable only to TCP based monitors. The secure option cannot be used with a CITRIX-AG monitor, because a CITRIX-AG monitor uses a secure connection by default.

Possible values: YES, NO Default value: NO

validateCred Validate the credentials of the Xen Desktop DDC server user. Applicable to monitors of type CITRIX-XD-DDC.

Possible values: YES, NO Default value: NO

domain Domain in which the XenDesktop Desktop Delivery Controller (DDC) servers or Web Interface servers are present. Required by CITRIX-XD-DDC and CITRIX-WI-EXTENDED monitors for logging on to the DDC servers and Web Interface servers, respectively.

IPAddress Set of IP addresses expected in the monitoring response from the DNS server, if the record type is A or AAAA. Applicable to DNS monitors.

group Name of a newsgroup available on the NNTP service that is to be monitored. The appliance periodically generates an NNTP query for the name of the newsgroup and evaluates the response. If the newsgroup is found on the server, the service is marked as UP. If the newsgroup does not exist or if the search fails, the service is marked as DOWN. Applicable to NNTP monitors.

fileName Name of a file on the FTP server. The appliance monitors the FTP service by periodically checking the existence of the file on the server. Applicable to FTP-EXTENDED monitors.

baseDN The base distinguished name of the LDAP service, from where the LDAP server can begin the search for the attributes in the monitoring query. Required for LDAP service monitoring.

bindDN The distinguished name with which an LDAP monitor can perform the Bind operation on the LDAP server. Optional. Applicable to LDAP monitors.

filter Filter criteria for the LDAP query. Optional.

attribute Attribute to evaluate when the LDAP server responds to the query. Success or failure of the monitoring probe depends on whether the attribute exists in the response. Optional.

database Name of the database to connect to during authentication.

oracleSid Name of the service identifier that is used to connect to the Oracle database during authentication.

sqlQuery SQL query for a MYSQL-ECV or MSSQL-ECV monitor. Sent to the database server after the server authenticates the connection.

evalRule Expression that evaluates the database server's response to a MYSQL-ECV or MSSQL-ECV monitoring query. Must produce a Boolean result. The result determines the state of the server. If the expression returns TRUE, the probe succeeds. For example, if you want the

appliance to evaluate the error message to determine the state of the server, use the rule MYSQL.RES.ROW(10) .TEXT_ELEM(2).EQ("MySQL").

mssqlProtocolVersion Version of MSSQL server that is to be monitored.

Possible values: 70, 2000, 2000SP1, 2005, 2008, 2008R2, 2012, 2014 Default value: 70

snmpOID SNMP OID for SNMP monitors.

snmpCommunity Community name for SNMP monitors.

snmpThreshold Threshold for SNMP monitors.

snmpVersion SNMP version to be used for SNMP monitors.

Possible values: V1, V2

metricTable Metric table to which to bind metrics.

application Name of the application used to determine the state of the service. Applicable to monitors of type CITRIX-XML-SERVICE.

sitePath URL of the logon page. For monitors of type CITRIX-WEB-INTERFACE, to monitor a dynamic page under the site path, terminate the site path with a slash (/). Applicable to CITRIX-WEB-INTERFACE, CITRIX-WI-EXTENDED and CITRIX-XDM monitors.

storename Store Name. For monitors of type STOREFRONT, STORENAME is an optional argument defining storefront service store name. Applicable to STOREFRONT monitors.

storefrontacctservice Enable/Disable probing for Account Service. Applicable only to Store Front monitors. For multi-tenancy configuration users my skip account service

Possible values: YES, NO Default value: YES

netProfile Name of the network profile.

originHost Origin-Host value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

originRealm Origin-Realm value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

hostIPAddress Host-IP-Address value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. If Host-IP-Address is not specified, the appliance inserts the

mapped IP (MIP) address or subnet IP (SNIP) address from which the CER request (the monitoring probe) is sent.

vendorId Vendor-Id value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. Minimum value: 0

productName Product-Name value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

firmwareRevision Firmware-Revision value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. Minimum value: 0

authApplicationId List of Auth-Application-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring CER message. Minimum value: 0 Maximum value: 4294967295

acctApplicationId List of Acct-Application-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring message. Minimum value: 0 Maximum value: 4294967295

inbandSecurityId Inband-Security-Id for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.

Possible values: NO_INBAND_SECURITY, TLS

supportedVendorIds List of Supported-Vendor-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum eight of these AVPs are supported in a monitoring message. Minimum value: 1 Maximum value: 4294967295

vendorSpecificVendorId Vendor-Id to use in the Vendor-Specific-Application-Id grouped attribute-value pair (AVP) in the monitoring CER message. To specify Auth-Application-Id or Acct-Application-Id in Vendor-Specific-Application-Id, use vendorSpecificAuthApplicationIds or vendorSpecificAcctApplicationIds, respectively. Only one Vendor-Id is supported for all the Vendor-Specific-Application-Id AVPs in a CER monitoring message. Minimum value: 1

vendorSpecificAuthApplicationIds List of Vendor-Specific-Auth-Application-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring message. The specified value is combined with the value of vendorSpecificVendorId to obtain the Vendor-

Specific-Application-Id AVP in the CER monitoring message. Minimum value: 0 Maximum value: 4294967295

vendorSpecificAcctApplicationIds List of Vendor-Specific-Acct-Application-Id attribute value pairs (AVPs) to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring message. The specified value is combined with the value of vendorSpecificVendorId to obtain the Vendor-Specific-Application-Id AVP in the CER monitoring message. Minimum value: 0 Maximum value: 4294967295

kcdAccount KCD Account used by MSSQL monitor

storedb Store the database list populated with the responses to monitor probes. Used in database specific load balancing if MSSQL-ECV/MYSQL-ECV monitor is configured.

Possible values: ENABLED, DISABLED Default value: DISABLED

storefrontcheckbackendservices This option will enable monitoring of services running on storefront server. Storefront services are monitored by probing to a Windows service that runs on the Storefront server and exposes details of which storefront services are running.

Possible values: YES, NO Default value: NO

trofscode Code expected when the server is under maintenance Minimum value: 0

trofsstring String expected from the server for the service to be marked as trofs. Applicable to HTTP-ECV/TCP-ECV monitors.

sslProfile SSL Profile associated with the monitor

mqttClientIdentifier Client id to be used in Connect command

mqttVersion Version of MQTT protocol used in connect message, default is version 3.1.1 Default value: 4 Minimum value: 3

grpcHealthCheck Option to enable or disable gRPC health check service.

Possible values: YES, NO Default value: NO

grpcStatusCode gRPC status codes for which to mark the service as UP. The default value is 12(health check unimplemented). If the gRPC status code 0 is received from the backend this configuration is ignored. Minimum value: 0

grpcServiceName Option to specify gRPC service name on which gRPC health check need to be performed

Example

add monitor http_mon http

enable lb monitor

Enable the monitor that is bound to a specific service. If no monitor name is specified, all monitors bound to the service are enabled.

Synopsis

enable lb monitor (<serviceName>@ | <serviceGroupName>@)

Arguments

serviceName The name of the service to which the monitor is bound.

serviceGroupName The name of the service group to which the monitor is to be bound.

monitorName Name for the monitor. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my monitor" or 'my monitor').

Example

enable monitor http_svc http_mon To enable monitor for multiple services use the following command: enable monitor http_svc http_mon

Related Commands

- add service

lb-parameter

The following operations can be performed on "lb-parameter":

show| unset| set|

show lb parameter

Displays the global load balancing parameters.

Synopsis

show lb parameter

Arguments

Output

httpOnlyCookieFlag Include the HttpOnly attribute in persistence cookies. The HttpOnly attribute limits the scope of a cookie to HTTP requests and helps mitigate the risk of cross-site scripting attacks.

useSecuredPersistenceCookie Encode persistence cookie values using SHA2 hash.

useEncryptedPersistenceCookie Encode persistence cookie values using SHA2 hash.

cookiePassphrase Use this parameter to specify the passphrase used to generate secured persistence cookie value. It specifies the passphrase with a maximum of 31 characters.

consolidatedLConn To find the service with the fewest connections, the virtual server uses the consolidated connection statistics from all the packet engines. The NO setting allows consideration of only the number of connections on the packet engine that received the new connection.

usePortForHashLb Include the port number of the service when creating a hash for hash based load balancing methods. With the NO setting, only the IP address of the service is considered when creating a hash.

preferDirectRoute Perform route lookup for traffic received by the Citrix ADC, and forward the traffic according to configured routes. Do not set this parameter if you want a wildcard virtual server to direct packets received by the appliance to an intermediary device, such as a firewall, even if their destination is directly connected to the appliance. Route lookup is performed after the packets have been processed and returned by the intermediary device.

startupRRFactor Used to change the factor of service hits after which vserver will come out of slowstart phase.

monitorSkipMaxClient When a monitor initiates a connection to a service, do not check to determine whether the number of connections to the service has reached the limit specified by the service's Max Clients setting. Enables monitoring to continue even if the service has reached its connection limit.

monitorConnectionClose Close monitoring connections by sending the service a connection termination message with the specified bit set.

vServerSpecificMac Allow a MAC-mode virtual server to accept traffic returned by an intermediary device, such as a firewall, to which the traffic was previously forwarded by another MAC-mode virtual server. The second virtual server can then distribute that traffic across the destination server farm. Also useful when load balancing Branch Repeater appliances. Note: The second virtual server can also send the traffic to another set of intermediary devices, such as another set of firewalls. If necessary, you can configure multiple MAC-mode virtual servers to pass traffic successively through multiple sets of intermediary devices.

sessionsThreshold This option is used to get the upper-limit on the number of persistent sessions set by the administrator for this system

builtin feature The feature to be checked while applying this config

AllowBoundSvcRemoval This is used, to enable/disable the option of svc/svcgroup removal, if it is bound to one or more vserver. If it is enabled, the svc/svcgroup can be removed, even if it bound to vservers. If disabled, an error will be thrown, when the user tries to remove a svc/svcgroup without unbinding from its vservers.

retainservicestate This option is used to retain the original state of service or servicegroup member when an enable server command is issued.

dbsTTL Specify the TTL for DNS record for domain based service. The default value of ttl is 0 which indicates to use the TTL received in DNS response for monitors

maxPipelineNat Maximum number of concurrent requests to allow on a single client connection, which is identified by the clientip:port-<vserver ip:port> tuple. This parameter is applicable to ANY service type and all UDP service types (except DNS) and only when "svrTimeout" is set to zero. A value of 0 (zero) applies no limit to the number of concurrent requests allowed on a single client connection

LiteralADCCookieAttribute String configured as LiteralADCCookieAttribute will be appended as attribute for Citrix ADC cookie (for example: LB cookie persistence , GSLB site persistence, CS cookie persistence, LB group cookie persistence).

Sample usage - set lb parameter -LiteralADCCookieAttribute ";SameSite=None"

ComputedADCCookieAttribute ComputedADCCookieAttribute accepts ns variable as input in form of string starting with $ (to understand how to configure ns variable, please check man add ns variable). policies can be configured to modify this variable for every transaction and the final value of the variable after policy evaluation will be appended as attribute to Citrix ADC cookie (for

example: LB cookie persistence , GSLB sitepersistence, CS cookie persistence, LB group cookie persistence). Only one of ComputedADCCookieAttribute, LiteralADCCookieAttribute can be set.

Sample usage - add ns variable lbvar -type TEXT(100) -scope Transaction add ns assignment lbassign -variable $lbvar -set "\\";SameSite=Strict\\"" add rewrite policy lbpol <valid policy expression> lbassign bind rewrite global lbpol 100 next -type RES_OVERRIDE set lb param -ComputedADCCookieAttribute "$lbvar" For incoming client request, if above policy evaluates TRUE, then SameSite=Strict will be appended to ADC generated cookie

ADCCookieAttributeWarningMsg Used to describe any configuration issue with respect to ns variable configured as part of set lb parameter

storeMqttClientidAndUsername This option allows to store the MQTT clientid and username in transactional logs

dropMqttJumboMessage When this option is enabled, MQTT messages of length greater than 64k will be dropped and the client/server connections will be reset.

lbHashAlgoWinSize This options allows to increase window size used in LB hashing algorithm(DEFAULT).

lbHashAlgorithm This option dictates the hashing algorithm used for hash based LB methods (URLHASH, DOMAINHASH, SOURCEIPHASH, DESTINATIONIPHASH, SRCIPDESTIPHASH, SRCIPSRCPORTHASH, TOKEN, USER_TOKEN, CALLIDHASH).

lbHashFingers This option is used to specify the number of fingers to be used in PRAC and JARH algorithms for hash based LB methods. Increasing the number of fingers might give better distribution of traffic at the expense of additional memory

undefAction Action to perform when policy evaluation creates an UNDEF condition. Available settings function as follows:

- NOLBACTION - Does not consider LB action in making LB decision.
- RESET - Reset the request and notify the user, so that the user can resend the request.
- DROP - Drop the request without sending a response to the user.

overridePersistencyforOrder This option is used to override persistency when order is configured for services or servicegroups.

proximityFromSelf Use the ADC location instead of client IP for static proximity LB or GSLB decision.

Example

show lb parameter

unset lb parameter

Use this command to remove lb parameter settings.Refer to the set lb parameter command for meanings of the arguments.

Synopsis

unset lb parameter

set lb parameter

Modifies the specified global load balancing parameters.

Synopsis

set lb parameter

Arguments

httpOnlyCookieFlag Include the HttpOnly attribute in persistence cookies. The HttpOnly attribute limits the scope of a cookie to HTTP requests and helps mitigate the risk of cross-site scripting attacks.

Possible values: ENABLED, DISABLED Default value: ENABLED

useEncryptedPersistenceCookie Encode persistence cookie values using SHA2 hash.

Possible values: ENABLED, DISABLED Default value: DISABLED

cookiePassphrase Use this parameter to specify the passphrase used to generate secured persistence cookie value. It specifies the passphrase with a maximum of 31 characters.

consolidatedLConn To find the service with the fewest connections, the virtual server uses the consolidated connection statistics from all the packet engines. The NO setting allows consideration of only the number of connections on the packet engine that received the new connection.

Possible values: YES, NO Default value: YES

usePortForHashLb Include the port number of the service when creating a hash for hash based load balancing methods. With the NO setting, only the IP address of the service is considered when creating a hash.

Possible values: YES, NO Default value: YES

preferDirectRoute Perform route lookup for traffic received by the Citrix ADC, and forward the traffic according to configured routes. Do not set this parameter if you want a wildcard virtual server to direct packets received by the appliance to an intermediary device, such as a firewall, even if their destination is directly connected to the appliance. Route lookup is performed after the packets have been processed and returned by the intermediary device.

Possible values: YES, NO Default value: YES

startupRRFactor Number of requests, per service, for which to apply the round robin load balancing method before switching to the configured load balancing method, thus allowing services to ramp up gradually to full load. Until the specified number of requests is distributed, the Citrix ADC is said to be implementing the slow start mode (or startup round robin). Implemented for a virtual server when one of the following is true:

- The virtual server is newly created.
- One or more services are newly bound to the virtual server.
- One or more services bound to the virtual server are enabled.
- The load balancing method is changed. This parameter applies to all the load balancing virtual servers configured on the Citrix ADC, except for those virtual servers for which the virtual server-level slow start parameters (New Service Startup Request Rate and Increment Interval) are configured. If the global slow start parameter and the slow start parameters for a given virtual server are not set, the appliance implements a default slow start for the virtual server, as follows:
- For a newly configured virtual server, the appliance implements slow start for the first 100 requests received by the virtual server.
- For an existing virtual server, if one or more services are newly bound or newly enabled, or if the load balancing method is changed, the appliance dynamically computes the number of requests for which to implement startup round robin. It obtains this number by multiplying the request rate by the number of bound services (it includes services that are marked as DOWN). For example, if the current request rate is 20 requests/s and ten services are bound to the virtual server, the appliance performs startup round robin for 200 requests. Not applicable to a virtual server for which a hash based load balancing method is configured. Minimum value: 0

monitorSkipMaxClient When a monitor initiates a connection to a service, do not check to determine whether the number of connections to the service has reached the limit specified by the

service's Max Clients setting. Enables monitoring to continue even if the service has reached its connection limit.

Possible values: ENABLED, DISABLED Default value: DISABLED

monitorConnectionClose Close monitoring connections by sending the service a connection termination message with the specified bit set.

Possible values: RESET, FIN Default value: FIN

vServerSpecificMac Allow a MAC-mode virtual server to accept traffic returned by an intermediary device, such as a firewall, to which the traffic was previously forwarded by another MAC-mode virtual server. The second virtual server can then distribute that traffic across the destination server farm. Also useful when load balancing Branch Repeater appliances. Note: The second virtual server can also send the traffic to another set of intermediary devices, such as another set of firewalls. If necessary, you can configure multiple MAC-mode virtual servers to pass traffic successively through multiple sets of intermediary devices.

Possible values: ENABLED, DISABLED Default value: DISABLED

AllowBoundSvcRemoval This is used, to enable/disable the option of svc/svcgroup removal, if it is bound to one or more vserver. If it is enabled, the svc/svcgroup can be removed, even if it bound to vservers. If disabled, an error will be thrown, when the user tries to remove a svc/svcgroup without unbinding from its vservers.

Possible values: ENABLED, DISABLED Default value: ENABLED

retainservicestate This option is used to retain the original state of service or servicegroup member when an enable server command is issued.

Possible values: ON, OFF Default value: OFF

dbsTTL Specify the TTL for DNS record for domain based service. The default value of ttl is 0 which indicates to use the TTL received in DNS response for monitors Default value: 0

maxPipelineNat Maximum number of concurrent requests to allow on a single client connection, which is identified by the clientip:port-<vserver ip:port> tuple. This parameter is applicable to ANY service type and all UDP service types (except DNS) and only when "svrTimeout" is set to zero. A value of 0 (zero) applies no limit to the number of concurrent requests allowed on a single client connection Default value: NSNATPCB_MAXPIPELINE Minimum value: 0

LiteralADCCookieAttribute String configured as LiteralADCCookieAttribute will be appended as attribute for Citrix ADC cookie (for example: LB cookie persistence , GSLB site persistence, CS cookie persistence, LB group cookie persistence).

Sample usage - set lb parameter -LiteralADCCookieAttribute ";SameSite=None"

ComputedADCCookieAttribute ComputedADCCookieAttribute accepts ns variable as input in form of string starting with $ (to understand how to configure ns variable, please check man add ns variable). policies can be configured to modify this variable for every transaction and the final value of the variable after policy evaluation will be appended as attribute to Citrix ADC cookie (for example: LB cookie persistence , GSLB sitepersistence, CS cookie persistence, LB group cookie persistence). Only one of ComputedADCCookieAttribute, LiteralADCCookieAttribute can be set.

Sample usage - add ns variable lbvar -type TEXT(100) -scope Transaction add ns assignment lbassign -variable $lbvar -set "\\";SameSite=Strict\\"" add rewrite policy lbpol <valid policy expression> lbassign bind rewrite global lbpol 100 next -type RES_OVERRIDE set lb param -ComputedADCCookieAttribute "$lbvar" For incoming client request, if above policy evaluates TRUE, then SameSite=Strict will be appended to ADC generated cookie

storeMqttClientidAndUsername This option allows to store the MQTT clientid and username in transactional logs

Possible values: YES, NO Default value: NO

dropMqttJumboMessage When this option is enabled, MQTT messages of length greater than 64k will be dropped and the client/server connections will be reset.

Possible values: YES, NO Default value: YES

lbHashAlgorithm This option dictates the hashing algorithm used for hash based LB methods (URLHASH, DOMAINHASH, SOURCEIPHASH, DESTINATIONIPHASH, SRCIPDESTIPHASH, SRCIPSRCPORTHASH, TOKEN, USER_TOKEN, CALLIDHASH).

Possible values: DEFAULT, PRAC, JARH Default value: DEFAULT

lbHashFingers This option is used to specify the number of fingers to be used in PRAC and JARH algorithms for hash based LB methods. Increasing the number of fingers might give better distribution of traffic at the expense of additional memory Default value: 256 Minimum value: 1 Maximum value: 1024

undefAction Action to perform when policy evaluation creates an UNDEF condition. Available settings function as follows:

- NOLBACTION - Does not consider LB action in making LB decision.
- RESET - Reset the request and notify the user, so that the user can resend the request.
- DROP - Drop the request without sending a response to the user. Default value: "NOLBACTION"

proximityFromSelf Use the ADC location instead of client IP for static proximity LB or GSLB decision.

Possible values: YES, NO Default value: NO

Example

set lb parameter -httponly (ENABLED|DISABLED)

lb-persistentSessions

The following operations can be performed on "lb-persistentSessions":

show| clear|

show lb persistentSessions

Get all vserver persistent sessions

Synopsis

show lb persistentSessions

Arguments

vServer The name of the virtual server.

Output

type Type of Persistence.

typestring Type of Persistence as String.

srcIP SOURCE IP.

srcIPv6 SOURCE IPv6 ADDRESS.

destIP DESTINATION IP.

destIPv6 DESTINATION IPv6 ADDRESS.

flags IPv6 FLAGS.

destPort Destination port.

vServerName Virtual server name.

timeout Persistent Session timeout.

referenceCount Reference Count.

sipCallID SIP CALLID.

persistenceParam Specific persistence information . Callid in case of SIP_CALLID persistence entry , RTSP session id in case of RTSP_SESSIONID persistence entry.

cnamePersparam The cname that is selected incase of gslb service

devno count stateflag

clear lb persistentSessions

Use this command to clear/flush persistent sessions

Synopsis

clear lb persistentSessions

Arguments

vServer The name of the LB vserver whose persistence sessions are to be flushed. If not specified, all persistence sessions will be flushed .

persistenceParameter The persistence parameter whose persistence sessions are to be flushed.

lb-policy

The following operations can be performed on "lb-policy":

stat| add| rename| show| unset| rm| set|

stat lb policy

Displays statistics for all the LB policies currently configured on the Citrix ADC, or detailed statistics for the specified policy.

Synopsis

stat lb policy

Arguments

name Name of the LB policy for which to show detailed statistics.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Policy undef hits (Undefhits) Number of undef hits on the policy

Related Commands

- stat lb policylabel

add lb policy

Creates an LB policy which specifies requests for which LB decision is taken based on order sequence specified in corresponding LB action

Synopsis

add lb policy <name> -rule <expression> -action <string>

Arguments

name Name of the LB policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the LB policy is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy" or 'my lb policy').

rule Expression against which traffic is evaluated.

action Name of action to use if the request matches this LB policy.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Available settings function as follows:

- NOLBACTION - Does not consider LB actions in making LB decision.
- RESET - Reset the request and notify the user, so that the user can resend the request.
- DROP - Drop the request without sending a response to the user.

logAction Name of the messagelog action to use for requests that match this policy.

comment Any type of information about this LB policy.

Example

add lb policy lbpol1 -rule CLIENT.IP.SRC.EQ(102.10.20.1) -action lbact1

rename lb policy

Renames the specified LB policy.

Synopsis

rename lb policy <name>@ <newName>@

Arguments

name Existing name of the LB policy.

newName New name for the LB policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy" or 'my lb policy').

Example

rename lb policy lbpol1 lbpol2

show lb policy

Displays the current settings for the specified LB policy.', If no policy name is specified, displays a list of all LB policies currently configured on the Citrix ADC, with abbreviated settings.

Synopsis

show lb policy show lb policy stats - alias for 'stat lb policy'

Arguments

name Name of the LB policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the LB policy is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy" or 'my lb policy').

Output

stateflag rule Expression against which traffic is evaluated.

action Name of action to use if the request matches this LB policy.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Available settings function as follows:

- NOLBACTION - Does not consider LB actions in making LB decision.
- RESET - Reset the request and notify the user, so that the user can resend the request.
- DROP - Drop the request without sending a response to the user.

hits Number of hits.

undefHits Number of policy UNDEF hits.

activePolicy Indicates whether policy is bound or not.

boundTo Location where policy is bound

priority Specifies the priority of the policy.

comment Any type of information about this LB policy.

bindPolicyType vserverType gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

feature The feature to be checked while applying this config

builtin Flag to determine if LB policy is built-in or not

type gslbBindings logAction Name of the messagelog action to use for requests that match this policy.

devno count

Example

show lb policy

unset lb policy

Use this command to remove lb policy settings.Refer to the set lb policy command for meanings of the arguments.

Synopsis

unset lb policy <name>

rm lb policy

Removes the specified LB policy.

Synopsis

rm lb policy <name>

Arguments

name Name of the LB policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the LB policy is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy" or 'my lb policy').

Example

rm lb policy lbpol1

set lb policy

Modifies the specified parameters of the LB policy.

Synopsis

set lb policy <name>

Arguments

name Name of the LB policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the LB policy is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy" or 'my lb policy').

rule Expression against which traffic is evaluated.

action Name of action to use if the request matches this LB policy.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Available settings function as follows:

- NOLBACTION - Does not consider LB actions in making LB decision.
- RESET - Reset the request and notify the user, so that the user can resend the request.
- DROP - Drop the request without sending a response to the user.

logAction Name of the messagelog action to use for requests that match this policy.

comment Any type of information about this LB policy.

Example

set lb policy lbpol1 -rule CLIENT.IP.SRC.EQ(102.10.20.2)

lb-policylabel

The following operations can be performed on "lb-policylabel":

stat| rename| rm| add| show| bind| unbind|

stat lb policylabel

Displays statistics for the specified LB policy label. If no policy label name is provided, displays abbreviated statistics for all the LB policy labels currently configured on the Citrix ADC.

Synopsis

stat lb policylabel

Arguments

labelName Name of the LB policy label.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy Label Hits (Hits) Number of times policy label was invoked.

Related Commands

- stat lb vserver

rename lb policylabel

Renames the specified LB policy label.

Synopsis

rename lb policylabel <labelName>@ <newName>@

Arguments

labelName Current name of the LB policy label.

newName New name for the LB policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

Example

rename lb policylabel oldname newname

rm lb policylabel

Removes the specified LB policy label.

Synopsis

rm lb policylabel <labelName>

Arguments

labelName Name for the LB policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy label" or 'my lb policy label').

Example

rm lb policylabel lblabel1

add lb policylabel

Creates a user-defined LB policy label, to which you can bind policies. A policy label is a tool for evaluating a set of policies in a specified order.

Synopsis

add lb policylabel <labelName>

Arguments

labelName Name for the LB policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy label" or 'my lb policy label').

policylabeltype Protocols supported by the policylabel. Available Types are :

- HTTP - HTTP requests.
- DNS - DNS request.
- OTHERTCP - OTHERTCP request.
- SIP_UDP - SIP_UDP request.
- SIP_TCP - SIP_TCP request.
- MYSQL - MYSQL request.
- MSSQL - MSSQL request.
- ORACLE - ORACLE request.
- NAT - NAT request.
- DIAMETER - DIAMETER request.
- RADIUS - RADIUS request.
- MQTT - MQTT request.
- QUIC_BRIDGE - QUIC_BRIDGE request.
- HTTP_QUIC - HTTP_QUIC request.

Possible values: HTTP, OTHERTCP, SIP_UDP, SIP_TCP, MYSQL, MSSQL, ORACLE, NAT, DIAMETER, RADIUS, DNS, MQTT, QUIC_BRIDGE, HTTP_QUIC Default value: HTTP

comment Any comments to preserve information about this LB policy label.

Example

add lb policylabel lblabel1

show lb policylabel

Displays the current settings for the specified LB policylabel. If no policy label is specified, displays a list of all the LB policy labels currently configured on the Citrix ADC, with abbreviated settings.

Synopsis

show lb policylabel

Arguments

labelName Name for the LB policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy label" or 'my lb policy label').

Output

policylabeltype Protocols supported by the policylabel. Available Types are :

- HTTP - HTTP requests.
- DNS - DNS request.
- OTHERTCP - OTHERTCP request.
- SIP_UDP - SIP_UDP request.
- SIP_TCP - SIP_TCP request.
- MYSQL - MYSQL request.
- MSSQL - MSSQL request.
- ORACLE - ORACLE request.
- NAT - NAT request.
- DIAMETER - DIAMETER request.
- RADIUS - RADIUS request.
- MQTT - MQTT request.
- QUIC_BRIDGE - QUIC_BRIDGE request.
- HTTP_QUIC - HTTP_QUIC request.

stateflag numpol number of polices bound to label.

hits Number of times policy label was invoked.

policyName Name of the LB policy.

priority Specifies the priority of the policy.

flags comment Any comments to preserve information about this LB policy label.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label and evaluate the specified policy label.

labelType Type of policy label to invoke. Available settings function as follows:

- vserver - Invokes the unnamed policy label associated with the specified virtual server.
- policylabel - Invoke a user-defined policy label.

labelName

- If labelType is policylabel, name of the policy label to invoke.
- If labelType is reqvserver, name of the virtual server.

devno count

Example

show lb policylabel lblabel1

bind lb policylabel

Binds the specified LB policy to the specified LB policylabel.

Synopsis

bind lb policylabel <labelName> -policyName <string> -priority <positive_integer>

Arguments

labelName Name for the LB policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy label" or 'my lb policy label').

policyName Name of the policy to bind to the LB policylabel.

priority Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Must be unique within the label. Policies are evaluated in the order of their priority numbers, and the first policy that matches the request is applied. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.
- The expression evaluates to a priority number that is smaller than the current policys priority number.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label and evaluate the specified policy label.

labelType Type of policy label to invoke. Available settings function as follows:

- vserver - Invokes the unnamed policy label associated with the specified virtual server.
- policylabel - Invoke a user-defined policy label.

Possible values: reqvserver, policylabel

labelName

- If labelType is policylabel, name of the policy label to invoke.
- If labelType is reqvserver, name of the virtual server.

Example

bind lb policylabel lblabel1 lbpol1 10

unbind lb policylabel

Unbinds the specified LB policy from the specified policy label.

Synopsis

unbind lb policylabel <labelName> -policyName <string>

Arguments

labelName Name for the LB policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy label" or 'my lb policy label').

policyName The name of the policy to be unbound.

Example

unbind lb policylabel lblabel1 lbpol1

lb-profile

The following operations can be performed on "lb-profile":

unset| show| rm| set| add|

unset lb profile

Use this command to remove lb profile settings.Refer to the set lb profile command for meanings of the arguments.

Synopsis

unset lb profile <lbprofilename>

show lb profile

Displays the list of lb profile/s in the device

Synopsis

show lb profile

Arguments

lbprofilename Name of the LB profile.

Output

dbsLb Enable database specific load balancing for MySQL and MSSQL service types.

processLocal By turning on this option packets destined to a vserver in a cluster will not under go any steering. Turn this option for single pa cket request response mode or when the upstream device is performing a proper RSS for connection based distribution.

httpOnlyCookieFlag Include the HttpOnly attribute in persistence cookies. The HttpOnly attribute limits the scope of a cookie to HTTP requests and helps mitigate the risk of cross-site scripting attacks.

cookiePassphrase Use this parameter to specify the passphrase used to generate secured persistence cookie value. It specifies the passphrase with a maximum of 31 characters.

useSecuredPersistenceCookie Encode persistence cookie values using SHA2 hash.

useEncryptedPersistenceCookie Encode persistence cookie values using SHA2 hash.

vsvrcount Total number of vservers , the profile is bound to

stateflag Flags controlling the display.

LiteralADCCookieAttribute String configured as LiteralADCCookieAttribute will be appended as attribute for Citrix ADC cookie (for example: LB cookie persistence , GSLB site persistence, CS cookie persistence, LB group cookie persistence).

Sample usage - add lb profile lbprof -LiteralADCCookieAttribute ";SameSite=None"

ComputedADCCookieAttribute ComputedADCCookieAttribute accepts ns variable as input in form of string starting with $ (to understand how to configure ns variable, please check man add ns variable). policies can be configured to modify this variable for every transaction and the final value of the variable after policy evaluation will be appended as attribute to Citrix ADC cookie (for example: LB cookie persistence , GSLB sitepersistence, CS cookie persistence, LB group cookie persistence). Only one of ComputedADCCookieAttribute, LiteralADCCookieAttribute can be set.

Sample usage - add ns variable lbvar -type TEXT(100) -scope Transaction add ns assignment lbassign -variable $lbvar -set "\\";SameSite=Strict\\"" add rewrite policy lbpol <valid policy expression> lbassign bind rewrite global lbpol 100 next -type RES_OVERRIDE add lb profile lbprof -ComputedADCCookieAttribute "$lbvar" For incoming client request, if above policy evaluates TRUE, then SameSite=Strict will be appended to ADC generated cookie

ADCCookieAttributeWarningMsg Used to describe any configuration issue with respect to ns variable configured as part of add/set lb profile

storeMqttClientidAndUsername This option allows to store the MQTT clientid and username in transactional logs

lbHashAlgoWinSize This options allows to increase window size used in LB hashing algorithm(DEFAULT).

lbHashAlgorithm This option dictates the hashing algorithm used for hash based LB methods (URLHASH, DOMAINHASH, SOURCEIPHASH, DESTINATIONIPHASH, SRCIPDESTIPHASH, SRCIPSRCPORTHASH, TOKEN, USER_TOKEN, CALLIDHASH).

lbHashFingers This option is used to specify the number of fingers to be used in PRAC and JARH algorithms for hash based LB methods. Increasing the number of fingers might give better distribution of traffic at the expense of additional memory.

proximityFromSelf Use the ADC location instead of client IP for static proximity LB or GSLB decision.

devno count

rm lb profile

Removes a LB profile from the device.

Synopsis

rm lb profile <lbprofilename>

Arguments

lbprofilename Name of the LB profile.

set lb profile

Modify the specific parameters of LB profile.

Synopsis

set lb profile <lbprofilename>

Arguments

lbprofilename Name of the LB profile.

dbsLb Enable database specific load balancing for MySQL and MSSQL service types.

Possible values: ENABLED, DISABLED Default value: DISABLED

processLocal By turning on this option packets destined to a vserver in a cluster will not under go any steering. Turn this option for single pa cket request response mode or when the upstream device is performing a proper RSS for connection based distribution.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpOnlyCookieFlag Include the HttpOnly attribute in persistence cookies. The HttpOnly attribute limits the scope of a cookie to HTTP requests and helps mitigate the risk of cross-site scripting attacks.

Possible values: ENABLED, DISABLED Default value: ENABLED

cookiePassphrase Use this parameter to specify the passphrase used to generate secured persistence cookie value. It specifies the passphrase with a maximum of 31 characters.

useEncryptedPersistenceCookie Encode persistence cookie values using SHA2 hash.

Possible values: ENABLED, DISABLED Default value: DISABLED

LiteralADCCookieAttribute String configured as LiteralADCCookieAttribute will be appended as attribute for Citrix ADC cookie (for example: LB cookie persistence , GSLB site persistence, CS cookie persistence, LB group cookie persistence).

Sample usage - add lb profile lbprof -LiteralADCCookieAttribute ";SameSite=None"

ComputedADCCookieAttribute ComputedADCCookieAttribute accepts ns variable as input in form of string starting with $ (to understand how to configure ns variable, please check man add ns variable). policies can be configured to modify this variable for every transaction and the final value of the variable after policy evaluation will be appended as attribute to Citrix ADC cookie (for example: LB cookie persistence , GSLB sitepersistence, CS cookie persistence, LB group cookie persistence). Only one of ComputedADCCookieAttribute, LiteralADCCookieAttribute can be set.

Sample usage - add ns variable lbvar -type TEXT(100) -scope Transaction add ns assignment lbassign -variable $lbvar -set "\\";SameSite=Strict\\"" add rewrite policy lbpol <valid policy expression> lbassign bind rewrite global lbpol 100 next -type RES_OVERRIDE add lb profile lbprof -ComputedADCCookieAttribute "$lbvar" For incoming client request, if above policy evaluates TRUE, then SameSite=Strict will be appended to ADC generated cookie

storeMqttClientidAndUsername This option allows to store the MQTT clientid and username in transactional logs

Possible values: YES, NO Default value: NO

lbHashAlgorithm This option dictates the hashing algorithm used for hash based LB methods (URLHASH, DOMAINHASH, SOURCEIPHASH, DESTINATIONIPHASH, SRCIPDESTIPHASH, SRCIPSRCPORTHASH, TOKEN, USER_TOKEN, CALLIDHASH).

Possible values: DEFAULT, PRAC, JARH Default value: DEFAULT

lbHashFingers This option is used to specify the number of fingers to be used in PRAC and JARH algorithms for hash based LB methods. Increasing the number of fingers might give better distribution of traffic at the expense of additional memory. Default value: 256 Minimum value: 1 Maximum value: 1024

proximityFromSelf Use the ADC location instead of client IP for static proximity LB or GSLB decision.

Possible values: YES, NO Default value: NO

add lb profile

Creates a LB profile.

Synopsis

add lb profile <lbprofilename>

Arguments

lbprofilename Name of the LB profile.

dbsLb Enable database specific load balancing for MySQL and MSSQL service types.

Possible values: ENABLED, DISABLED Default value: DISABLED

processLocal By turning on this option packets destined to a vserver in a cluster will not under go any steering. Turn this option for single pa cket request response mode or when the upstream device is performing a proper RSS for connection based distribution.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpOnlyCookieFlag Include the HttpOnly attribute in persistence cookies. The HttpOnly attribute limits the scope of a cookie to HTTP requests and helps mitigate the risk of cross-site scripting attacks.

Possible values: ENABLED, DISABLED Default value: ENABLED

cookiePassphrase Use this parameter to specify the passphrase used to generate secured persistence cookie value. It specifies the passphrase with a maximum of 31 characters.

useEncryptedPersistenceCookie Encode persistence cookie values using SHA2 hash.

Possible values: ENABLED, DISABLED Default value: DISABLED

LiteralADCCookieAttribute String configured as LiteralADCCookieAttribute will be appended as attribute for Citrix ADC cookie (for example: LB cookie persistence , GSLB site persistence, CS cookie persistence, LB group cookie persistence).

Sample usage - add lb profile lbprof -LiteralADCCookieAttribute ";SameSite=None"

ComputedADCCookieAttribute ComputedADCCookieAttribute accepts ns variable as input in form of string starting with $ (to understand how to configure ns variable, please check man add ns variable). policies can be configured to modify this variable for every transaction and the final value of the variable after policy evaluation will be appended as attribute to Citrix ADC cookie (for

example: LB cookie persistence , GSLB sitepersistence, CS cookie persistence, LB group cookie persistence). Only one of ComputedADCCookieAttribute, LiteralADCCookieAttribute can be set.

Sample usage - add ns variable lbvar -type TEXT(100) -scope Transaction add ns assignment lbassign -variable $lbvar -set "\\";SameSite=Strict\\"" add rewrite policy lbpol <valid policy expression> lbassign bind rewrite global lbpol 100 next -type RES_OVERRIDE add lb profile lbprof -ComputedADCCookieAttribute "$lbvar" For incoming client request, if above policy evaluates TRUE, then SameSite=Strict will be appended to ADC generated cookie

storeMqttClientidAndUsername This option allows to store the MQTT clientid and username in transactional logs

Possible values: YES, NO Default value: NO

lbHashAlgorithm This option dictates the hashing algorithm used for hash based LB methods (URLHASH, DOMAINHASH, SOURCEIPHASH, DESTINATIONIPHASH, SRCIPDESTIPHASH, SRCIPSRCPORTHASH, TOKEN, USER_TOKEN, CALLIDHASH).

Possible values: DEFAULT, PRAC, JARH Default value: DEFAULT

lbHashFingers This option is used to specify the number of fingers to be used in PRAC and JARH algorithms for hash based LB methods. Increasing the number of fingers might give better distribution of traffic at the expense of additional memory. Default value: 256 Minimum value: 1 Maximum value: 1024

proximityFromSelf Use the ADC location instead of client IP for static proximity LB or GSLB decision.

Possible values: YES, NO Default value: NO

lb-route

The following operations can be performed on "lb-route":

show| add| rm|

show lb route

Display the names of the routes associated to the route structure using the ###add lb route### command.

Synopsis

show lb route [<network> <netmask>]

Arguments

network The destination network or host.

netmask The netmask of the destination network.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Default value: 0 Minimum value: 0 Maximum value: 4094

Output

gatewayName The name of the route.

flags State of the configured gateway.

devno count stateflag

add lb route

Bind the route VIP to the route structure.

Synopsis

add lb route <network> <netmask> <gatewayName>

Arguments

network The IP address of the network to which the route belongs.

netmask The netmask to which the route belongs.

gatewayName The name of the route.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Default value: 0 Minimum value: 0 Maximum value: 4094

rm lb route

Remove the route VIP from the route structure.

Synopsis

rm lb route <network> <netmask>

Arguments

network The IP address of the network to which the route VIP belongs.

netmask The netmask of the destination network.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Default value: 0 Minimum value: 0 Maximum value: 4094

lb-route6

The following operations can be performed on "lb-route6":

add| show| rm|

add lb route6

Bind the route VIP to the route structure.

Synopsis

add lb route6 <network> <gatewayName>

Arguments

network The destination network.

gatewayName The name of the route.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Default value: 0 Minimum value: 0 Maximum value: 4094

show lb route6

Display the names of the routes associated to the route structure using the ###add lb route6### command.

Synopsis

show lb route6 [<network>]

Arguments

network The destination network or host.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Default value: 0 Minimum value: 0 Maximum value: 4094

Output

gatewayName The name of the route.

flags State of the configured gateway.

devno count stateflag

rm lb route6

Remove the route VIP from the route structure.

Synopsis

rm lb route6 <network>

Arguments

network The IP address of the network to which the route VIP belongs.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Default value: 0 Minimum value: 0 Maximum value: 4094

lb-sipParameters

The following operations can be performed on "lb-sipParameters":

set| show| unset|

set lb sipParameters

Modifies the specified global SIP parameters.

Synopsis

set lb sipParameters

Arguments

rnatSrcPort Port number with which to match the source port in server-initiated SIP traffic. The rport parameter is added, without a value, to SIP packets that have a matching source port number, and CALL-ID based persistence is implemented for the responses received by the virtual server. Default value: 0

rnatDstPort Port number with which to match the destination port in server-initiated SIP traffic. The rport parameter is added, without a value, to SIP packets that have a matching destination port number, and CALL-ID based persistence is implemented for the responses received by the virtual server. Default value: 0

retryDur Time, in seconds, for which a client must wait before initiating a connection after receiving a 503 Service Unavailable response from the SIP server. The time value is sent in the "Retry-After" header in the 503 response. Default value: 120 Minimum value: 1

addRportVip Add the rport parameter to the VIA headers of SIP requests that virtual servers receive from clients or servers.

Possible values: ENABLED, DISABLED Default value: ENABLED

sip503RateThreshold Maximum number of 503 Service Unavailable responses to generate, once every 10 milliseconds, when a SIP virtual server becomes unavailable. Default value: 100 Minimum value: 0

rnatsecuresrcport Port number with which to match the source port in server-initiated SIP over SSL traffic. The rport parameter is added, without a value, to SIP packets that have a matching source port number, and CALL-ID based persistence is implemented for the responses received by the virtual server. Default value: 0

rnatsecuredstport Port number with which to match the destination port in server-initiated SIP over SSL traffic. The rport parameter is added, without a value, to SIP packets that have a matching destination port number, and CALL-ID based persistence is implemented for the responses received by the virtual server. Default value: 0

Example

set sip parameter

show lb sipParameters

Displays the global SIP parameters.

Synopsis

show lb sipParameters

Arguments

Output

rnatSrcPort Port number with which to match the source port in server-initiated SIP traffic. The rport parameter is added, without a value, to SIP packets that have a matching source port number, and CALL-ID based persistence is implemented for the responses received by the virtual server.

rnatDstPort Port number with which to match the destination port in server-initiated SIP traffic. The rport parameter is added, without a value, to SIP packets that have a matching destination port number, and CALL-ID based persistence is implemented for the responses received by the virtual server.

retryDur Time, in seconds, for which a client must wait before initiating a connection after receiving a 503 Service Unavailable response from the SIP server. The time value is sent in the "Retry-After" header in the 503 response.

addRportVip Add the rport parameter to the VIA headers of SIP requests that virtual servers receive from clients or servers.

sip503RateThreshold Maximum number of 503 Service Unavailable responses to generate, once every 10 milliseconds, when a SIP virtual server becomes unavailable.

rnatsecuresrcport Port number with which to match the source port in server-initiated SIP over SSL traffic. The rport parameter is added, without a value, to SIP packets that have a matching source port number, and CALL-ID based persistence is implemented for the responses received by the virtual server.

rnatsecuredstport Port number with which to match the destination port in server-initiated SIP over SSL traffic. The rport parameter is added, without a value, to SIP packets that have a matching destination port number, and CALL-ID based persistence is implemented for the responses received by the virtual server.

builtin Flag to determine if SIP param is built-in or not

feature The feature to be checked while applying this config

Example

show sip parameter

unset lb sipParameters

Use this command to remove lb sipParameters settings.Refer to the set lb sipParameters command for meanings of the arguments.

Synopsis

unset lb sipParameters

lb-vserver

The following operations can be performed on "lb-vserver":

bind| add| unbind| disable| set| enable| show| rename| rm| unset| stat|

bind lb vserver

Binds a service, service group, or policy to a virtual server.

Synopsis

bind lb vserver <name>@ ((<serviceName>@) | <serviceGroupName>@ | (-policyName <string>@) | -analyticsProfile <string>@)

Arguments

name Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver').

serviceName Name of the service.

weight Integer specifying the weight of the service. A larger number specifies a greater weight. Defines the capacity of the service relative to the other services in the load balancing configuration. Determines the priority given to the service in load balancing decisions. Default value: 1 Minimum value: 1 Maximum value: 100

serviceGroupName Name of the service group.

policyName Name of the policy to bind to the virtual server.

priority Integer specifying the policy's priority. The lower the priority number, the higher the policy's priority. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

type Bind point to which to bind the policy.

Possible values: REQUEST, RESPONSE, MQTT_JUMBO_REQ

invoke Invoke policies bound to a virtual server or policy label.

labelType Type of policy label to invoke. Applicable only to rewrite, videooptimization and cache policies. Available settings function as follows:

- reqvserver - Evaluate the request against the request-based policies bound to the specified virtual server.
- resvserver - Evaluate the response against the response-based policies bound to the specified virtual server.
- policylabel - invoke the request or response against the specified user-defined policy label.

Possible values: reqvserver, resvserver, policylabel

labelName Name of the virtual server or user-defined policy label to invoke if the policy evaluates to TRUE.

analyticsProfile bind lb vserver <vserver_name> -analyticsProfile <analytics-profile-name>.

order Integer specifying the order of the service. A larger number specifies a lower order. Defines the order of the service relative to the other services in the load balancing vserver's bindings. Determines the priority given to the service among all the services bound. Minimum value: 1 Maximum value: 8192

Example

bind lb vserver http_vip http_svc To bind a service to multiple vservers use the following command: bind lb vs http_vip http_svc To bind multiple services to a vserver use the following command: bind lb vs http_vip http_svc

add lb vserver

Creates a load balancing virtual server.

Synopsis

add lb vserver <name>@ <serviceType> [-lbMethod <lbMethod>] [-Listenpolicy <expression>] [-insertVserverIPPort <insertVserverIPPort>] [-newServiceRequest <positive_integer>] [-redirectFromPort <port|*>] [-probeProtocol (TCP | HTTP)]

Arguments

name Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space,

colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver').

serviceType Protocol used by the service (also called the service type).

Possible values: HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, DNS, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, TFTP, ORACLE, SMPP, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, PROXY, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, MONGO, MONGO_TLS, MQTT, MQTT_TLS, QUIC_BRIDGE, HTTP_QUIC

IPAddress IPv4 or IPv6 address to assign to the virtual server.

IPPattern IP address pattern, in dotted decimal notation, for identifying packets to be accepted by the virtual server. The IP Mask parameter specifies which part of the destination IP address is matched against the pattern. Mutually exclusive with the IP Address parameter. For example, if the IP pattern assigned to the virtual server is 198.51.100.0 and the IP mask is 255.255.240.0 (a forward mask), the first 20 bits in the destination IP addresses are matched with the first 20 bits in the pattern. The virtual server accepts requests with IP addresses that range from 198.51.96.1 to 198.51.111.254. You can also use a pattern such as 0.0.2.2 and a mask such as 0.0.255.255 (a reverse mask). If a destination IP address matches more than one IP pattern, the pattern with the longest match is selected, and the associated virtual server processes the request. For example, if virtual servers vs1 and vs2 have the same IP pattern, 0.0.100.128, but different IP masks of 0.0.255.255 and 0.0.224.255, a destination IP address of 198.51.100.128 has the longest match with the IP pattern of vs1. If a destination IP address matches two or more virtual servers to the same extent, the request is processed by the virtual server whose port number matches the port number in the request.

IPMask IP mask, in dotted decimal notation, for the IP Pattern parameter. Can have leading or trailing non-zero octets (for example, 255.255.240.0 or 0.0.255.255). Accordingly, the mask specifies whether the first n bits or the last n bits of the destination IP address in a client request are to be matched with the corresponding bits in the IP pattern. The former is called a forward mask. The latter is called a reverse mask.

port Port number for the virtual server.

ipset The list of IPv4/IPv6 addresses bound to ipset would form a part of listening service on the current lb vserver

range Number of IP addresses that the appliance must generate and assign to the virtual server. The virtual server then functions as a network virtual server, accepting traffic on any of the generated IP addresses. The IP addresses are generated automatically, as follows:

- For a range of n, the last octet of the address specified by the IP Address parameter increments n-1 times.
- If the last octet exceeds 255, it rolls over to 0 and the third octet increments by 1. Note: The Range parameter assigns multiple IP addresses to one virtual server. To generate an array of virtual servers, each of which owns only one IP address, use brackets in the IP Address and Name parameters to specify the range. For example: add lb vserver my_vserver HTTP 192.0.2. 80 Default value: 1 Minimum value: 1 Maximum value: 254

persistenceType Type of persistence for the virtual server. Available settings function as follows:

- SOURCEIP - Connections from the same client IP address belong to the same persistence session.
- COOKIEINSERT - Connections that have the same HTTP Cookie, inserted by a Set-Cookie directive from a server, belong to the same persistence session.
- SSLSESSION - Connections that have the same SSL Session ID belong to the same persistence session.
- CUSTOMSERVERID - Connections with the same server ID form part of the same session. For this persistence type, set the Server ID (CustomServerID) parameter for each service and configure the Rule parameter to identify the server ID in a request.
- RULE - All connections that match a user defined rule belong to the same persistence session.
- URLPASSIVE - Requests that have the same server ID in the URL query belong to the same persistence session. The server ID is the hexadecimal representation of the IP address and port of the service to which the request must be forwarded. This persistence type requires a rule to identify the server ID in the request.
- DESTIP - Connections to the same destination IP address belong to the same persistence session.
- SRCIPDESTIP - Connections that have the same source IP address and destination IP address belong to the same persistence session.
- CALLID - Connections that have the same CALL-ID SIP header belong to the same persistence session.
- RTSPSID - Connections that have the same RTSP Session ID belong to the same persistence session.

- FIXSESSION - Connections that have the same SenderCompID and TargetCompID values belong to the same persistence session.
- USERSESSION - Persistence session is created based on the persistence parameter value provided from an extension.

Possible values: SOURCEIP, COOKIEINSERT, SSLSESSION, RULE, URLPASSIVE, CUSTOMSERVERID, DESTIP, SRCIPDESTIP, CALLID, RTSPSID, DIAMETER, FIXSESSION, USERSESSION, NONE

timeout Time period for which a persistence session is in effect. Default value: 2 Maximum value: 1440

persistenceBackup Backup persistence type for the virtual server. Becomes operational if the primary persistence mechanism fails.

Possible values: SOURCEIP, NONE

backupPersistenceTimeout Time period for which backup persistence is in effect. Default value: 2 Minimum value: 2 Maximum value: 1440

lbMethod Load balancing method. The available settings function as follows:

- ROUNDROBIN - Distribute requests in rotation, regardless of the load. Weights can be assigned to services to enforce weighted round robin distribution.
- LEASTCONNECTION (default) - Select the service with the fewest connections.
- LEASTRESPONSETIME - Select the service with the lowest average response time.
- LEASTBANDWIDTH - Select the service currently handling the least traffic.
- LEASTPACKETS - Select the service currently serving the lowest number of packets per second.
- CUSTOMLOAD - Base service selection on the SNMP metrics obtained by custom load monitors.
- LRTM - Select the service with the lowest response time. Response times are learned through monitoring probes. This method also takes the number of active connections into account. Also available are a number of hashing methods, in which the appliance extracts a predetermined portion of the request, creates a hash of the portion, and then checks whether any previous requests had the same hash value. If it finds a match, it forwards the request to the service that served those previous requests. Following are the hashing methods:
- URLHASH - Create a hash of the request URL (or part of the URL).

- DOMAINHASH - Create a hash of the domain name in the request (or part of the domain name). The domain name is taken from either the URL or the Host header. If the domain name appears in both locations, the URL is preferred. If the request does not contain a domain name, the load balancing method defaults to LEASTCONNECTION.
- DESTINATIONIPHASH - Create a hash of the destination IP address in the IP header.
- SOURCEIPHASH - Create a hash of the source IP address in the IP header.
- TOKEN - Extract a token from the request, create a hash of the token, and then select the service to which any previous requests with the same token hash value were sent.
- SRCIPDESTIPHASH - Create a hash of the string obtained by concatenating the source IP address and destination IP address in the IP header.
- SRCIPSRCPORTHASH - Create a hash of the source IP address and source port in the IP header.
- CALLIDHASH - Create a hash of the SIP Call-ID header.
- USER_TOKEN - Same as TOKEN LB method but token needs to be provided from an extension.

Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, URLHASH, DOMAINHASH, DESTINATIONIPHASH, SOURCEIPHASH, SRCIPDESTIPHASH, LEASTBANDWIDTH, LEASTPACKETS, TOKEN, SRCIPSRCPORTHASH, LRTM, CALLIDHASH, CUSTOMLOAD, LEASTREQUEST, AUDITLOGHASH, STATICPROXIMITY, USER_TOKEN
Default value: LEASTCONNECTION

hashLength Number of bytes to consider for the hash value used in the URLHASH and DOMAINHASH load balancing methods. Default value: 80 Minimum value: 1 Maximum value: 4096

netmask IPv4 subnet mask to apply to the destination IP address or source IP address when the load balancing method is DESTINATIONIPHASH or SOURCEIPHASH. Default value: 0xFFFFFFFF

v6netmasklen Number of bits to consider in an IPv6 destination or source IP address, for creating the hash that is required by the DESTINATIONIPHASH and SOURCEIPHASH load balancing methods. Default value: 128 Minimum value: 1 Maximum value: 128

backupLBMethod Backup load balancing method. Becomes operational if the primary load balancing me thod fails or cannot be used. Valid only if the primary method is based on static proximity.

Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, CUSTOMLOAD Default value: ROUNDROBIN

cookieName Use this parameter to specify the cookie name for COOKIE peristence type. It specifies the name of cookie with a maximum of 32 characters. If not specified, cookie name is internally generated.

rule Expression, or name of a named expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Default value: "none"

Listenpolicy Expression identifying traffic accepted by the virtual server. Can be either an expression (for example, CLIENT.IP.DST.IN_SUBNET(192.0.2.0/24) or the name of a named expression. In the above example, the virtual server accepts all requests whose destination IP address is in the 192.0.2.0/24 subnet. Default value: "NONE"

Listenpriority Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server the virtual server whose listen policy has the highest priority (the lowest priority number) accepts the request. Default value: 101 Minimum value: 0 Maximum value: 101

resRule Expression specifying which part of a server's response to use for creating rule based persistence sessions (persistence type RULE). Can be either an expression or the name of a named expression. Example: HTTP.RES.HEADER("setcookie").VALUE(0).TYPECAST_NVLIST_T('=',';').VALUE("server1"). Default value: "none"

persistMask Persistence mask for IP based persistence types, for IPv4 virtual servers. Default value: 0xFFFFFFFF

v6persistmasklen Persistence mask for IP based persistence types, for IPv6 virtual servers. Default value: 128 Minimum value: 1 Maximum value: 128

rtspNat Use network address translation (NAT) for RTSP data connections.

Possible values: ON, OFF Default value: OFF

m Redirection mode for load balancing. Available settings function as follows:

- IP - Before forwarding a request to a server, change the destination IP address to the server's IP address.
- MAC - Before forwarding a request to a server, change the destination MAC address to the server's MAC address. The destination IP address is not changed. MAC-based redirection mode is used mostly in firewall load balancing deployments.
- IPTUNNEL - Perform IP-in-IP encapsulation for client IP packets. In the outer IP headers, set the destination IP address to the IP address of the server and the source IP address to the subnet IP (SNIP). The client IP packets are not modified. Applicable to both IPv4 and IPv6 packets.
- TOS - Encode the virtual server's TOS ID in the TOS field of the IP header. You can use either the IPTUNNEL or the TOS option to implement Direct Server Return (DSR).

Possible values: IP, MAC, IPTUNNEL, TOS Default value: IP

tosId TOS ID of the virtual server. Applicable only when the load balancing redirection mode is set to TOS. Minimum value: 1 Maximum value: 63

dataLength Length of the token to be extracted from the data segment of an incoming packet, for use in the token method of load balancing. The length of the token, specified in bytes, must not be greater than 24 KB. Applicable to virtual servers of type TCP. Minimum value: 1 Maximum value: 100

dataOffset Offset to be considered when extracting a token from the TCP payload. Applicable to virtual servers, of type TCP, using the token method of load balancing. Must be within the first 24 KB of the TCP payload. Minimum value: 0 Maximum value: 25400

sessionless Perform load balancing on a per-packet basis, without establishing sessions. Recommended for load balancing of intrusion detection system (IDS) servers and scenarios involving direct server return (DSR), where session information is unnecessary.

Possible values: ENABLED, DISABLED Default value: DISABLED

trofsPersistence When value is ENABLED, Trofs persistence is honored. When value is DISABLED, Trofs persistence is not honored.

Possible values: ENABLED, DISABLED Default value: ENABLED

state State of the load balancing virtual server.

Possible values: ENABLED, DISABLED Default value: ENABLED

connfailover Mode in which the connection failover feature must operate for the virtual server. After a failover, established TCP connections and UDP packet flows are kept active and resumed on the secondary appliance. Clients remain connected to the same servers. Available settings function as follows:

- STATEFUL - The primary appliance shares state information with the secondary appliance, in real time, resulting in some runtime processing overhead.
- STATELESS - State information is not shared, and the new primary appliance tries to re-create the packet flow on the basis of the information contained in the packets it receives.
- DISABLED - Connection failover does not occur.

Possible values: DISABLED, STATEFUL, STATELESS Default value: DISABLED

redirectURL URL to which to redirect traffic if the virtual server becomes unavailable. WARNING! Make sure that the domain in the URL does not match the domain specified for a content switching policy. If it does, requests are continuously redirected to the unavailable virtual server.

cacheable Route cacheable requests to a cache redirection virtual server. The load balancing virtual server can forward requests only to a transparent cache redirection virtual server that has an IP address and port combination of *:80, so such a cache redirection virtual server must be configured on the appliance.

Possible values: YES, NO Default value: NO

cltTimeout Idle time, in seconds, after which a client connection is terminated. Default value: -1 Maximum value: 31536000

soMethod Type of threshold that, when exceeded, triggers spillover. Available settings function as follows:

- CONNECTION - Spillover occurs when the number of client connections exceeds the threshold.
- DYNAMICCONNECTION - Spillover occurs when the number of client connections at the virtual server exceeds the sum of the maximum client (Max Clients) settings for bound services. Do not specify a spillover threshold for this setting, because the threshold is implied by the Max Clients settings of bound services.

- BANDWIDTH - Spillover occurs when the bandwidth consumed by the virtual server's incoming and outgoing traffic exceeds the threshold.
- HEALTH - Spillover occurs when the percentage of weights of the services that are UP drops below the threshold. For example, if services svc1, svc2, and svc3 are bound to a virtual server, with weights 1, 2, and 3, and the spillover threshold is 50%, spillover occurs if svc1 and svc3 or svc2 and svc3 transition to DOWN.
- NONE - Spillover does not occur.

Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soPersistence If spillover occurs, maintain source IP address based persistence for both primary and backup virtual servers.

Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeOut Timeout for spillover persistence, in minutes. Default value: 2 Minimum value: 2 Maximum value: 1440

healthThreshold Threshold in percent of active services below which vserver state is made down. If this threshold is 0, vserver state will be up even if one bound service is up. Default value: 0 Minimum value: 0 Maximum value: 100

soThreshold Threshold at which spillover occurs. Specify an integer for the CONNECTION spillover method, a bandwidth value in kilobits per second for the BANDWIDTH method (do not enter the units), or a percentage for the HEALTH method (do not enter the percentage symbol). Minimum value: 1 Maximum value: 4294967287

soBackupAction Action to be performed if spillover is to take effect, but no backup chain to spillover is usable or exists

Possible values: DROP, ACCEPT, REDIRECT

redirectPortRewrite Rewrite the port and change the protocol to ensure successful HTTP redirects from services.

Possible values: ENABLED, DISABLED Default value: DISABLED

downStateFlush Flush all active transactions associated with a virtual server whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions.

Possible values: ENABLED, DISABLED Default value: ENABLED

backupVServer Name of the backup virtual server to which to forward requests if the primary virtual server goes DOWN or reaches its spillover threshold.

disablePrimaryOnDown If the primary virtual server goes down, do not allow it to return to primary status until manually enabled.

Possible values: ENABLED, DISABLED Default value: DISABLED

insertVserverIPPort Insert an HTTP header, whose value is the IP address and port number of the virtual server, before forwarding a request to the server. The format of the header is <vipHeader>: <virtual server IP address>_<port number >, where vipHeader is the name that you specify for the header. If the virtual server has an IPv6 address, the address in the header is enclosed in brackets () to separate it from the port number. If you have mapped an IPv4 address to a virtual server's IPv6 address, the value of this parameter determines which IP address is inserted in the header, as follows:

- VIPADDR - Insert the IP address of the virtual server in the HTTP header regardless of whether the virtual server has an IPv4 address or an IPv6 address. A mapped IPv4 address, if configured, is ignored.
- V6TOV4MAPPING - Insert the IPv4 address that is mapped to the virtual server's IPv6 address. If a mapped IPv4 address is not configured, insert the IPv6 address.
- OFF - Disable header insertion.

Possible values: OFF, VIPADDR, V6TOV4MAPPING

vipHeader Name for the inserted header. The default name is vip-header.

AuthenticationHost Fully qualified domain name (FQDN) of the authentication virtual server to which the user must be redirected for authentication. Make sure that the Authentication parameter is set to ENABLED.

Authentication Enable or disable user authentication.

Possible values: ON, OFF Default value: OFF

authn401 Enable or disable user authentication with HTTP 401 responses.

Possible values: ON, OFF Default value: OFF

authnVsName Name of an authentication virtual server with which to authenticate users.

push Process traffic with the push virtual server that is bound to this load balancing virtual server.

Possible values: ENABLED, DISABLED Default value: DISABLED

pushVserver Name of the load balancing virtual server, of type PUSH or SSL_PUSH, to which the server pushes updates received on the load balancing virtual server that you are configuring.

pushLabel Expression for extracting a label from the server's response. Can be either an expression or the name of a named expression. Default value: "none"

pushMultiClients Allow multiple Web 2.0 connections from the same client to connect to the virtual server and expect updates.

Possible values: YES, NO Default value: NO

tcpProfileName Name of the TCP profile whose settings are to be applied to the virtual server.

httpProfileName Name of the HTTP profile whose settings are to be applied to the virtual server.

dbProfileName Name of the DB profile whose settings are to be applied to the virtual server.

comment Any comments that you might want to associate with the virtual server.

l2Conn Use Layer 2 parameters (channel number, MAC address, and VLAN ID) in addition to the 4-tuple (<source IP>:<source port>::<destination IP>:<destination port>) that is used to identify a connection. Allows multiple TCP and non-TCP connections with the same 4-tuple to co-exist on the Citrix ADC.

Possible values: ON, OFF

oracleServerVersion Oracle server version

Possible values: 10G, 11G Default value: 10G

mssqlServerVersion For a load balancing virtual server of type MSSQL, the Microsoft SQL Server version. Set this parameter if you expect some clients to run a version different from the version of the database. This setting provides compatibility between the client-side and server-side connections by ensuring that all communication conforms to the server's version.

Possible values: 70, 2000, 2000SP1, 2005, 2008, 2008R2, 2012, 2014 Default value: 2008R2

mysqlProtocolVersion MySQL protocol version that the virtual server advertises to clients. Default value: NSA_MYSQL_PROTOCOL_VER_DEFAULT Minimum value: 0

mysqlServerVersion MySQL server version string that the virtual server advertises to clients. Default value: NSA_MYSQL_SERVER_VER_DEFAULT

mysqlCharacterSet Character set that the virtual server advertises to clients. Default value: NSA_MYSQL_CHAR_SET_DEFAULT Minimum value: 0

mysqlServerCapabilities Server capabilities that the virtual server advertises to clients. Default value: NSA_MYSQL_SVR_CAPABILITIES_DEFAULT Minimum value: 0

appflowLog Apply AppFlow logging to the virtual server.

Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile Name of the network profile to associate with the virtual server. If you set this parameter, the virtual server uses only the IP addresses in the network profile as source IP addresses when initiating connections with servers.

icmpVsrResponse How the Citrix ADC responds to ping requests received for an IP address that is common to one or more virtual servers. Available settings function as follows:

- If set to PASSIVE on all the virtual servers that share the IP address, the appliance always responds to the ping requests.
- If set to ACTIVE on all the virtual servers that share the IP address, the appliance responds to the ping requests if at least one of the virtual servers is UP. Otherwise, the appliance does not respond.
- If set to ACTIVE on some virtual servers and PASSIVE on the others, the appliance responds if at least one virtual server with the ACTIVE setting is UP. Otherwise, the appliance does not respond. Note: This parameter is available at the virtual server level. A similar parameter, ICMP Response, is available at the IP address level, for IPv4 addresses of type VIP. To set that parameter, use the add ip command in the CLI or the Create IP dialog box in the GUI.

Possible values: PASSIVE, ACTIVE Default value: PASSIVE

RHIstate Route Health Injection (RHI) functionality of the NetSaler appliance for advertising the route of the VIP address associated with the virtual server. When Vserver RHI Level (RHI) parameter is set to VSVR_CNTRLD, the following are different RHI behaviors for the VIP address on the basis of RHIstate (RHI STATE) settings on the virtual servers associated with the VIP address:

- If you set RHI STATE to PASSIVE on all virtual servers, the Citrix ADC always advertises the route for the VIP address.
- If you set RHI STATE to ACTIVE on all virtual servers, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers is in UP state.

- If you set RHI STATE to ACTIVE on some and PASSIVE on others, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers, whose RHI STATE set to ACTIVE, is in UP state.

Possible values: PASSIVE, ACTIVE Default value: PASSIVE

newServiceRequest Number of requests, or percentage of the load on existing services, by which to increase the load on a new service at each interval in slow-start mode. A non-zero value indicates that slow-start is applicable. A zero value indicates that the global RR startup parameter is applied. Changing the value to zero will cause services currently in slow start to take the full traffic as determined by the LB method. Subsequently, any new services added will use the global RR factor. Default value: 0 Minimum value: 0

newServiceRequestUnit Units in which to increment load at each interval in slow-start mode.

Possible values: PER_SECOND, PERCENT Default value: PER_SECOND

newServiceRequestIncrementInterval Interval, in seconds, between successive increments in the load on a new service or a service whose state has just changed from DOWN to UP. A value of 0 (zero) specifies manual slow start. Default value: 0 Minimum value: 0 Maximum value: 3600

minAutoscaleMembers Minimum number of members expected to be present when vserver is used in Autoscale. Default value: 0 Minimum value: 0 Maximum value: 5000

maxAutoscaleMembers Maximum number of members expected to be present when vserver is used in Autoscale. Default value: 0 Minimum value: 0 Maximum value: 5000

persistAVPno Persist AVP number for Diameter Persistency. In case this AVP is not defined in Base RFC 3588 and it is nested inside a Grouped AVP, define a sequence of AVP numbers (max 3) in order of parent to child. So say persist AVP number X is nested inside AVP Y which is nested in Z, then define the list as Z Y X Minimum value: 1

skippersistency This argument decides the behavior incase the service which is selected from an existing persistence session has reached threshold.

Possible values: Bypass, ReLb, None Default value: None

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

authnProfile Name of the authentication profile to be used when authentication is turned on.

macmodeRetainvlan This option is used to retain vlan information of incoming packet when macmode is enabled

Possible values: ENABLED, DISABLED Default value: DISABLED

dbsLb Enable database specific load balancing for MySQL and MSSQL service types.

Possible values: ENABLED, DISABLED Default value: DISABLED

dns64 This argument is for enabling/disabling the dns64 on lbvserver

Possible values: ENABLED, DISABLED

bypassAAAA If this option is enabled while resolving DNS64 query AAAA queries are not sent to back end dns server

Possible values: YES, NO Default value: NO

RecursionAvailable When set to YES, this option causes the DNS replies from this vserver to have the RA bit turned on. Typically one would set this option to YES, when the vserver is load balancing a set of DNS servers thatsupport recursive queries.

Possible values: YES, NO Default value: NO

processLocal By turning on this option packets destined to a vserver in a cluster will not under go any steering. Turn this option for single packet request response mode or when the upstream device is performing a proper RSS for connection based distribution.

Possible values: ENABLED, DISABLED Default value: DISABLED

dnsProfileName Name of the DNS profile to be associated with the VServer. DNS profile properties will be applied to the transactions processed by a VServer. This parameter is valid only for DNS and DNS-TCP VServers.

lbprofilename Name of the LB profile which is associated to the vserver

redirectFromPort Port number for the virtual server, from which we absorb the traffic for http redirect Minimum value: 1

httpsRedirectUrl URL to which all HTTP traffic received on the port specified in the -redirectFromPort parameter is redirected.

retainConnectionsOnCluster This option enables you to retain existing connections on a node joining a Cluster system or when a node is being configured for passive timeout. By default, this option is disabled.

Possible values: YES, NO Default value: NO

adfsProxyProfile Name of the adfsProxy profile to be used to support ADFSPIP protocol for ADFS servers.

quicProfileName Name of QUIC profile which will be attached to the VServer.

quicBridgeProfilename Name of the QUIC Bridge profile whose settings are to be applied to the virtual server.

probeProtocol Citrix ADC provides support for external health check of the vserver status. Select HTTP or TCP probes for healthcheck

Possible values: TCP, HTTP

probeSuccessResponseCode HTTP code to return in SUCCESS case. Default value: "200 OK"

probePort Citrix ADC provides support for external health check of the vserver status. Select port for HTTP/TCP monitring Default value: 0

toggleorder Configure this option to toggle order preference

Possible values: ASCENDING, DESCENDING Default value: ASCENDING

orderthreshold This option is used to to specify the threshold of minimum number of services to be UP in an order, for it to be considered in Lb decision. Default value: 0 Minimum value: 0 Maximum value: 100

Example

add lb vserver http_vsvr http 10.102.1.10 80 To add multiple vservers at once use the following command: add lb vs http_vsvr http 10.102.27. 80 This command adds the vserver http_vsvr1 with the IP address 10.102.27.115, http_vsvr2 with 10.102.27.116, http_vsvr3 with 10.102.27.117 and http_vsvr4 with 10.102.27.118

unbind lb vserver

Unbinds a service, service group, or policy from a virtual server.

Synopsis

unbind lb vserver <name>@ (<serviceName>@ | <serviceGroupName>@ | (-policyName <string>@))

Arguments

name Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver').

serviceName Name of the service.

serviceGroupName The name of the service group that is unbound.

policyName Name of the policy to bind to the virtual server.

type Bind point from which to unbind the policy label.

Possible values: REQUEST, RESPONSE, MQTT_JUMBO_REQ

priority Priority number of the policy. Minimum value: 1 Maximum value: 2147483647

analyticsProfile unbind lb vserver <vserver_name> -analyticsProfile <analytics-profile-name>.

Example

unbind lb vserver http_vip http_svc To unbind a service from multiple vservers use the following command: unbind lb vs http_vip http_svc To unbind multiple services from a vserver use the following command: unbind lb vs http_vip http_svc

disable lb vserver

Disables a virtual server.

Synopsis

disable lb vserver <name>@

Arguments

name Name of the virtual server.

Example

disable vserver lb_vip To disable multiple vservers at once use the following command: disable vserver lb_vip

set lb vserver

Modifies the specified parameters of a load balancing virtual server.

Synopsis

set lb vserver <name>@ [<serviceName>@] [-lbMethod <lbMethod>] [-insertVserverIPPort <insertVserverIPPort>] [-probeProtocol (TCP | HTTP)]

Arguments

name Name of the virtual server.

IPAddress IPv4 or IPv6 address to assign to the virtual server.

ipset The list of IPv4/IPv6 addresses bound to ipset would form a part of listening service on the current lb vserver

IPPattern IP address pattern, in dotted decimal notation, for identifying packets to be accepted by the virtual server. The IP Mask parameter specifies which part of the destination IP address is matched against the pattern. Mutually exclusive with the IP Address parameter. For example, if the IP pattern assigned to the virtual server is 198.51.100.0 and the IP mask is 255.255.240.0 (a forward mask), the first 20 bits in the destination IP addresses are matched with the first 20 bits in the pattern. The virtual server accepts requests with IP addresses that range from 198.51.96.1 to 198.51.111.254. You can also use a pattern such as 0.0.2.2 and a mask such as 0.0.255.255 (a reverse mask). If a destination IP address matches more than one IP pattern, the pattern with the longest match is selected, and the associated virtual server processes the request. For example, if virtual servers vs1 and vs2 have the same IP pattern, 0.0.100.128, but different IP masks of 0.0.255.255 and 0.0.224.255, a destination IP address of 198.51.100.128 has the longest match with the IP pattern of vs1. If a destination IP address matches two or more virtual servers to the same extent, the request is processed by the virtual server whose port number matches the port number in the request.

IPMask IP mask, in dotted decimal notation, for the IP Pattern parameter. Can have leading or trailing non-zero octets (for example, 255.255.240.0 or 0.0.255.255). Accordingly, the mask specifies whether the first n bits or the last n bits of the destination IP address in a client request

are to be matched with the corresponding bits in the IP pattern. The former is called a forward mask. The latter is called a reverse mask.

serviceName Service to bind to the virtual server.

weight Weight to assign to the specified service. Minimum value: 1 Maximum value: 100

order Order number to be assigned to the service when it is bound to the lb vserver. Minimum value: 1 Maximum value: 8192

persistenceType Type of persistence for the virtual server. Available settings function as follows:

- SOURCEIP - Connections from the same client IP address belong to the same persistence session.
- COOKIEINSERT - Connections that have the same HTTP Cookie, inserted by a Set-Cookie directive from a server, belong to the same persistence session.
- SSLSESSION - Connections that have the same SSL Session ID belong to the same persistence session.
- CUSTOMSERVERID - Connections with the same server ID form part of the same session. For this persistence type, set the Server ID (CustomServerID) parameter for each service and configure the Rule parameter to identify the server ID in a request.
- RULE - All connections that match a user defined rule belong to the same persistence session.
- URLPASSIVE - Requests that have the same server ID in the URL query belong to the same persistence session. The server ID is the hexadecimal representation of the IP address and port of the service to which the request must be forwarded. This persistence type requires a rule to identify the server ID in the request.
- DESTIP - Connections to the same destination IP address belong to the same persistence session.
- SRCIPDESTIP - Connections that have the same source IP address and destination IP address belong to the same persistence session.
- CALLID - Connections that have the same CALL-ID SIP header belong to the same persistence session.
- RTSPSID - Connections that have the same RTSP Session ID belong to the same persistence session.
- FIXSESSION - Connections that have the same SenderCompID and TargetCompID values belong to the same persistence session.

- USERSESSION - Persistence session is created based on the persistence parameter value provided from an extension.

Possible values: SOURCEIP, COOKIEINSERT, SSLSESSION, RULE, URLPASSIVE, CUSTOMSERVERID, DESTIP, SRCIPDESTIP, CALLID, RTSPSID, DIAMETER, FIXSESSION, USERSESSION, NONE

timeout Time period for which a persistence session is in effect. Default value: 2 Maximum value: 1440

persistenceBackup Backup persistence type for the virtual server. Becomes operational if the primary persistence mechanism fails.

Possible values: SOURCEIP, NONE

backupPersistenceTimeout Time period for which backup persistence is in effect. Default value: 2 Minimum value: 2 Maximum value: 1440

lbMethod Load balancing method. The available settings function as follows:

- ROUNDROBIN - Distribute requests in rotation, regardless of the load. Weights can be assigned to services to enforce weighted round robin distribution.
- LEASTCONNECTION (default) - Select the service with the fewest connections.
- LEASTRESPONSETIME - Select the service with the lowest average response time.
- LEASTBANDWIDTH - Select the service currently handling the least traffic.
- LEASTPACKETS - Select the service currently serving the lowest number of packets per second.
- CUSTOMLOAD - Base service selection on the SNMP metrics obtained by custom load monitors.
- LRTM - Select the service with the lowest response time. Response times are learned through monitoring probes. This method also takes the number of active connections into account. Also available are a number of hashing methods, in which the appliance extracts a predetermined portion of the request, creates a hash of the portion, and then checks whether any previous requests had the same hash value. If it finds a match, it forwards the request to the service that served those previous requests. Following are the hashing methods:
- URLHASH - Create a hash of the request URL (or part of the URL).
- DOMAINHASH - Create a hash of the domain name in the request (or part of the domain name). The domain name is taken from either the URL or the Host header. If the domain name

appears in both locations, the URL is preferred. If the request does not contain a domain name, the load balancing method defaults to LEASTCONNECTION.

- DESTINATIONIPHASH - Create a hash of the destination IP address in the IP header.
- SOURCEIPHASH - Create a hash of the source IP address in the IP header.
- TOKEN - Extract a token from the request, create a hash of the token, and then select the service to which any previous requests with the same token hash value were sent.
- SRCIPDESTIPHASH - Create a hash of the string obtained by concatenating the source IP address and destination IP address in the IP header.
- SRCIPSRCPORTHASH - Create a hash of the source IP address and source port in the IP header.
- CALLIDHASH - Create a hash of the SIP Call-ID header.
- USER_TOKEN - Same as TOKEN LB method but token needs to be provided from an extension.

Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, URLHASH, DOMAINHASH, DESTINATIONIPHASH, SOURCEIPHASH, SRCIPDESTIPHASH, LEASTBANDWIDTH, LEASTPACKETS, TOKEN, SRCIPSRCPORTHASH, LRTM, CALLIDHASH, CUSTOMLOAD, LEASTREQUEST, AUDITLOGHASH, STATICPROXIMITY, USER_TOKEN
Default value: LEASTCONNECTION

hashLength Number of bytes to consider for the hash value used in the URLHASH and DOMAINHASH load balancing methods. Default value: 80 Minimum value: 1 Maximum value: 4096

netmask IPv4 subnet mask to apply to the destination IP address or source IP address when the load balancing method is DESTINATIONIPHASH or SOURCEIPHASH. Default value: 0xFFFFFFFF

v6netmasklen Number of bits to consider in an IPv6 destination or source IP address, for creating the hash that is required by the DESTINATIONIPHASH and SOURCEIPHASH load balancing methods. Default value: 128 Minimum value: 1 Maximum value: 128

backupLBMethod Backup load balancing method. Becomes operational if the primary load balancing me thod fails or cannot be used. Valid only if the primary method is based on static proximity.

Possible values: ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, CUSTOMLOAD Default value: ROUNDROBIN

rule Expression, or name of a named expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Default value: "none"

cookieName Use this parameter to specify the cookie name for COOKIE peristence type. It specifies the name of cookie with a maximum of 32 characters. If not specified, cookie name is internally generated.

resRule Expression specifying which part of a server's response to use for creating rule based persistence sessions (persistence type RULE). Can be either an expression or the name of a named expression. Example: HTTP.RES.HEADER("setcookie").VALUE(0).TYPECAST_NVLIST_T('=',';').VALUE("server1"). Default value: "none"

persistMask Persistence mask for IP based persistence types, for IPv4 virtual servers. Default value: 0xFFFFFFFF

v6persistmasklen Persistence mask for IP based persistence types, for IPv6 virtual servers. Default value: 128 Minimum value: 1 Maximum value: 128

rtspNat Use network address translation (NAT) for RTSP data connections.

Possible values: ON, OFF Default value: OFF

m Redirection mode for load balancing. Available settings function as follows:

- IP - Before forwarding a request to a server, change the destination IP address to the server's IP address.
- MAC - Before forwarding a request to a server, change the destination MAC address to the server's MAC address. The destination IP address is not changed. MAC-based redirection mode is used mostly in firewall load balancing deployments.

- IPTUNNEL - Perform IP-in-IP encapsulation for client IP packets. In the outer IP headers, set the destination IP address to the IP address of the server and the source IP address to the subnet IP (SNIP). The client IP packets are not modified. Applicable to both IPv4 and IPv6 packets.
- TOS - Encode the virtual server's TOS ID in the TOS field of the IP header. You can use either the IPTUNNEL or the TOS option to implement Direct Server Return (DSR).

Possible values: IP, MAC, IPTUNNEL, TOS Default value: IP

tosId TOS ID of the virtual server. Applicable only when the load balancing redirection mode is set to TOS. Minimum value: 1 Maximum value: 63

dataLength Length of the token to be extracted from the data segment of an incoming packet, for use in the token method of load balancing. The length of the token, specified in bytes, must not be greater than 24 KB. Applicable to virtual servers of type TCP. Minimum value: 1 Maximum value: 100

dataOffset Offset to be considered when extracting a token from the TCP payload. Applicable to virtual servers, of type TCP, using the token method of load balancing. Must be within the first 24 KB of the TCP payload. Minimum value: 0 Maximum value: 25400

sessionless Perform load balancing on a per-packet basis, without establishing sessions. Recommended for load balancing of intrusion detection system (IDS) servers and scenarios involving direct server return (DSR), where session information is unnecessary.

Possible values: ENABLED, DISABLED Default value: DISABLED

trofsPersistence When value is ENABLED, Trofs persistence is honored. When value is DISABLED, Trofs persistence is not honored.

Possible values: ENABLED, DISABLED Default value: ENABLED

connfailover Mode in which the connection failover feature must operate for the virtual server. After a failover, established TCP connections and UDP packet flows are kept active and resumed on the secondary appliance. Clients remain connected to the same servers. Available settings function as follows:

- STATEFUL - The primary appliance shares state information with the secondary appliance, in real time, resulting in some runtime processing overhead.
- STATELESS - State information is not shared, and the new primary appliance tries to re-create the packet flow on the basis of the information contained in the packets it receives.

- DISABLED - Connection failover does not occur.

Possible values: DISABLED, STATEFUL, STATELESS Default value: DISABLED

backupVServer Name of the backup virtual server to which to forward requests if the primary virtual server goes DOWN or reaches its spillover threshold.

redirectURL URL to which to redirect traffic if the virtual server becomes unavailable. WARNING! Make sure that the domain in the URL does not match the domain specified for a content switching policy. If it does, requests are continuously redirected to the unavailable virtual server.

cacheable Route cacheable requests to a cache redirection virtual server. The load balancing virtual server can forward requests only to a transparent cache redirection virtual server that has an IP address and port combination of *:80, so such a cache redirection virtual server must be configured on the appliance.

Possible values: YES, NO Default value: NO

cltTimeout Idle time, in seconds, after which a client connection is terminated. Default value: -1 Maximum value: 31536000

soMethod Type of threshold that, when exceeded, triggers spillover. Available settings function as follows:

- CONNECTION - Spillover occurs when the number of client connections exceeds the threshold.
- DYNAMICCONNECTION - Spillover occurs when the number of client connections at the virtual server exceeds the sum of the maximum client (Max Clients) settings for bound services. Do not specify a spillover threshold for this setting, because the threshold is implied by the Max Clients settings of bound services.
- BANDWIDTH - Spillover occurs when the bandwidth consumed by the virtual server's incoming and outgoing traffic exceeds the threshold.
- HEALTH - Spillover occurs when the percentage of weights of the services that are UP drops below the threshold. For example, if services svc1, svc2, and svc3 are bound to a virtual server, with weights 1, 2, and 3, and the spillover threshold is 50%, spillover occurs if svc1 and svc3 or svc2 and svc3 transition to DOWN.
- NONE - Spillover does not occur.

Possible values: CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, NONE

soThreshold Threshold at which spillover occurs. Specify an integer for the CONNECTION spillover method, a bandwidth value in kilobits per second for the BANDWIDTH method (do not enter the units), or a percentage for the HEALTH method (do not enter the percentage symbol). Minimum value: 1 Maximum value: 4294967287

soPersistence If spillover occurs, maintain source IP address based persistence for both primary and backup virtual servers.

Possible values: ENABLED, DISABLED Default value: DISABLED

soPersistenceTimeOut Timeout for spillover persistence, in minutes. Default value: 2 Minimum value: 2 Maximum value: 1440

healthThreshold Threshold in percent of active services below which vserver state is made down. If this threshold is 0, vserver state will be up even if one bound service is up. Default value: 0 Minimum value: 0 Maximum value: 100

soBackupAction Action to be performed if spillover is to take effect, but no backup chain to spillover is usable or exists

Possible values: DROP, ACCEPT, REDIRECT

redirectPortRewrite Rewrite the port and change the protocol to ensure successful HTTP redirects from services.

Possible values: ENABLED, DISABLED Default value: DISABLED

downStateFlush Flush all active transactions associated with a virtual server whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions.

Possible values: ENABLED, DISABLED Default value: ENABLED

insertVserverIPPort Insert an HTTP header, whose value is the IP address and port number of the virtual server, before forwarding a request to the server. The format of the header is <vipHeader>: <virtual server IP address>_<port number >, where vipHeader is the name that you specify for the header. If the virtual server has an IPv6 address, the address in the header is enclosed in brackets () to separate it from the port number. If you have mapped an IPv4 address to a virtual server's IPv6 address, the value of this parameter determines which IP address is inserted in the header, as follows:

- VIPADDR - Insert the IP address of the virtual server in the HTTP header regardless of whether the virtual server has an IPv4 address or an IPv6 address. A mapped IPv4 address, if configured, is ignored.
- V6TOV4MAPPING - Insert the IPv4 address that is mapped to the virtual server's IPv6 address. If a mapped IPv4 address is not configured, insert the IPv6 address.
- OFF - Disable header insertion.

Possible values: OFF, VIPADDR, V6TOV4MAPPING

vipHeader Name for the inserted header. The default name is vip-header.

disablePrimaryOnDown If the primary virtual server goes down, do not allow it to return to primary status until manually enabled.

Possible values: ENABLED, DISABLED Default value: DISABLED

AuthenticationHost Fully qualified domain name (FQDN) of the authentication virtual server to which the user must be redirected for authentication. Make sure that the Authentication parameter is set to ENABLED.

Authentication Enable or disable user authentication.

Possible values: ON, OFF Default value: OFF

authn401 Enable or disable user authentication with HTTP 401 responses.

Possible values: ON, OFF Default value: OFF

authnVsName Name of an authentication virtual server with which to authenticate users.

push Process traffic with the push virtual server that is bound to this load balancing virtual server.

Possible values: ENABLED, DISABLED Default value: DISABLED

pushVserver Name of the load balancing virtual server, of type PUSH or SSL_PUSH, to which the server pushes updates received on the load balancing virtual server that you are configuring.

pushLabel Expression for extracting a label from the server's response. Can be either an expression or the name of a named expression. Default value: "none"

pushMultiClients Allow multiple Web 2.0 connections from the same client to connect to the virtual server and expect updates.

Possible values: YES, NO Default value: NO

Listenpolicy Expression identifying traffic accepted by the virtual server. Can be either an expression (for example, CLIENT.IP.DST.IN_SUBNET(192.0.2.0/24) or the name of a named expression. In the above example, the virtual server accepts all requests whose destination IP address is in the 192.0.2.0/24 subnet. Default value: "NONE"

Listenpriority Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server the virtual server whose listen policy has the highest priority (the lowest priority number) accepts the request. Default value: 101 Minimum value: 0 Maximum value: 101

tcpProfileName Name of the TCP profile whose settings are to be applied to the virtual server.

httpProfileName Name of the HTTP profile whose settings are to be applied to the virtual server.

dbProfileName Name of the DB profile whose settings are to be applied to the virtual server.

comment Any comments that you might want to associate with the virtual server.

l2Conn Use Layer 2 parameters (channel number, MAC address, and VLAN ID) in addition to the 4-tuple (<source IP>:<source port>::<destination IP>:<destination port>) that is used to identify a connection. Allows multiple TCP and non-TCP connections with the same 4-tuple to co-exist on the Citrix ADC.

Possible values: ON, OFF

oracleServerVersion Oracle server version

Possible values: 10G, 11G Default value: 10G

mssqlServerVersion For a load balancing virtual server of type MSSQL, the Microsoft SQL Server version. Set this parameter if you expect some clients to run a version different from the version of the database. This setting provides compatibility between the client-side and server-side connections by ensuring that all communication conforms to the server's version.

Possible values: 70, 2000, 2000SP1, 2005, 2008, 2008R2, 2012, 2014 Default value: 2008R2

mysqlProtocolVersion MySQL protocol version that the virtual server advertises to clients. Default value: NSA_MYSQL_PROTOCOL_VER_DEFAULT Minimum value: 0

mysqlServerVersion MySQL server version string that the virtual server advertises to clients. Default value: NSA_MYSQL_SERVER_VER_DEFAULT

mysqlCharacterSet Character set that the virtual server advertises to clients. Default value: NSA_MYSQL_CHAR_SET_DEFAULT Minimum value: 0

mysqlServerCapabilities Server capabilities that the virtual server advertises to clients. Default value: NSA_MYSQL_SVR_CAPABILITIES_DEFAULT Minimum value: 0

appflowLog Apply AppFlow logging to the virtual server.

Possible values: ENABLED, DISABLED Default value: ENABLED

netProfile Name of the network profile to associate with the virtual server. If you set this parameter, the virtual server uses only the IP addresses in the network profile as source IP addresses when initiating connections with servers.

icmpVsrResponse How the Citrix ADC responds to ping requests received for an IP address that is common to one or more virtual servers. Available settings function as follows:

- If set to PASSIVE on all the virtual servers that share the IP address, the appliance always responds to the ping requests.
- If set to ACTIVE on all the virtual servers that share the IP address, the appliance responds to the ping requests if at least one of the virtual servers is UP. Otherwise, the appliance does not respond.
- If set to ACTIVE on some virtual servers and PASSIVE on the others, the appliance responds if at least one virtual server with the ACTIVE setting is UP. Otherwise, the appliance does not respond. Note: This parameter is available at the virtual server level. A similar parameter, ICMP Response, is available at the IP address level, for IPv4 addresses of type VIP. To set that parameter, use the add ip command in the CLI or the Create IP dialog box in the GUI.

Possible values: PASSIVE, ACTIVE Default value: PASSIVE

RHIstate Route Health Injection (RHI) functionality of the NetSaler appliance for advertising the route of the VIP address associated with the virtual server. When Vserver RHI Level (RHI) parameter is set to VSVR_CNTRLD, the following are different RHI behaviors for the VIP address on the basis of RHIstate (RHI STATE) settings on the virtual servers associated with the VIP address:

- If you set RHI STATE to PASSIVE on all virtual servers, the Citrix ADC always advertises the route for the VIP address.
- If you set RHI STATE to ACTIVE on all virtual servers, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers is in UP state.

- If you set RHI STATE to ACTIVE on some and PASSIVE on others, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers, whose RHI STATE set to ACTIVE, is in UP state.

Possible values: PASSIVE, ACTIVE Default value: PASSIVE

newServiceRequest Number of requests, or percentage of the load on existing services, by which to increase the load on a new service at each interval in slow-start mode. A non-zero value indicates that slow-start is applicable. A zero value indicates that the global RR startup parameter is applied. Changing the value to zero will cause services currently in slow start to take the full traffic as determined by the LB method. Subsequently, any new services added will use the global RR factor. Default value: 0 Minimum value: 0

newServiceRequestUnit Units in which to increment load at each interval in slow-start mode.

Possible values: PER_SECOND, PERCENT Default value: PER_SECOND

newServiceRequestIncrementInterval Interval, in seconds, between successive increments in the load on a new service or a service whose state has just changed from DOWN to UP. A value of 0 (zero) specifies manual slow start. Default value: 0 Minimum value: 0 Maximum value: 3600

minAutoscaleMembers Minimum number of members expected to be present when vserver is used in Autoscale. Default value: 0 Minimum value: 0 Maximum value: 5000

maxAutoscaleMembers Maximum number of members expected to be present when vserver is used in Autoscale. Default value: 0 Minimum value: 0 Maximum value: 5000

persistAVPno Persist AVP number for Diameter Persistency. In case this AVP is not defined in Base RFC 3588 and it is nested inside a Grouped AVP, define a sequence of AVP numbers (max 3) in order of parent to child. So say persist AVP number X is nested inside AVP Y which is nested in Z, then define the list as Z Y X Minimum value: 1

skippersistency This argument decides the behavior incase the service which is selected from an existing persistence session has reached threshold.

Possible values: Bypass, ReLb, None Default value: None

authnProfile Name of the authentication profile to be used when authentication is turned on.

macmodeRetainvlan This option is used to retain vlan information of incoming packet when macmode is enabled

Possible values: ENABLED, DISABLED Default value: DISABLED

dbsLb Enable database specific load balancing for MySQL and MSSQL service types.

Possible values: ENABLED, DISABLED Default value: DISABLED

dns64 This argument is for enabling/disabling the dns64 on lbvserver

Possible values: ENABLED, DISABLED

bypassAAAA If this option is enabled while resolving DNS64 query AAAA queries are not sent to back end dns server

Possible values: YES, NO Default value: NO

RecursionAvailable When set to YES, this option causes the DNS replies from this vserver to have the RA bit turned on. Typically one would set this option to YES, when the vserver is load balancing a set of DNS servers thatsupport recursive queries.

Possible values: YES, NO Default value: NO

processLocal By turning on this option packets destined to a vserver in a cluster will not under go any steering. Turn this option for single packet request response mode or when the upstream device is performing a proper RSS for connection based distribution.

Possible values: ENABLED, DISABLED Default value: DISABLED

dnsProfileName Name of the DNS profile to be associated with the VServer. DNS profile properties will be applied to the transactions processed by a VServer. This parameter is valid only for DNS and DNS-TCP VServers.

lbprofilename Name of the LB profile which is associated to the vserver

redirectFromPort Port number for the virtual server, from which we absorb the traffic for http redirect Minimum value: 1

httpsRedirectUrl URL to which all HTTP traffic received on the port specified in the -redirectFromPort parameter is redirected.

retainConnectionsOnCluster This option enables you to retain existing connections on a node joining a Cluster system or when a node is being configured for passive timeout. By default, this option is disabled.

Possible values: YES, NO Default value: NO

adfsProxyProfile Name of the adfsProxy profile to be used to support ADFSPIP protocol for ADFS servers.

quicProfileName Name of QUIC profile which will be attached to the VServer.

quicBridgeProfilename Name of the QUIC Bridge profile whose settings are to be applied to the virtual server.

probePort Citrix ADC provides support for external health check of the vserver status. Select port for HTTP/TCP monitring Default value: 0

probeProtocol Citrix ADC provides support for external health check of the vserver status. Select HTTP or TCP probes for healthcheck

Possible values: TCP, HTTP

probeSuccessResponseCode HTTP code to return in SUCCESS case. Default value: "200 OK"

toggleorder Configure this option to toggle order preference

Possible values: ASCENDING, DESCENDING Default value: ASCENDING

orderthreshold This option is used to to specify the threshold of minimum number of services to be UP in an order, for it to be considered in Lb decision. Default value: 0 Minimum value: 0 Maximum value: 100

Example

set lb vserver http_vip -lbmethod LEASTRESPONSETIME To set the load balancing method for multiple vserver use the following command: set lb vserver http_vip -lbmethod LEASTRESPONSETIME

enable lb vserver

Enables a virtual server.

Synopsis

enable lb vserver <name>@

Arguments

name Name of the virtual server.

Example

enable vserver lb_vip To enable multiple vservers at once use the following command: enable vserver lb_vip

show lb vserver

Displays the statistical data collected for a load balancing virtual server.

Synopsis

show lb vserver show lb vserver stats - alias for 'stat lb vserver'

Arguments

name Name of the virtual server. If no name is provided, statistical data of all configured virtual servers is displayed.

Output

insertVserverIPPort The virtual IP and port header insertion option for the vserver.

vipHeader Name for the inserted header. The default name is vip-header.

value SSL status.

stateflag appfwPolicyFlag IPAddress The IP address of the virtual server.

IPAddress IPv4 or IPv6 address to assign to the virtual server.

IPPattern The IP pattern of the virtual server.

IPMask The IP address mask of the virtual server.

Listenpolicy The string is listenpolicy configured for lb vserver

Listenpriority This parameter is the priority for listen policy of LB Vserver.

IPMapping The permanent mapping for the V6 Address

port Port number for the virtual server.

ipset The list of IPv4/IPv6 addresses bound to ipset would form a part of listening service on the current lb vserver

range Number of IP addresses that the appliance must generate and assign to the virtual server. The virtual server then functions as a network virtual server, accepting traffic on any of the generated IP addresses. The IP addresses are generated automatically, as follows:

- For a range of n, the last octet of the address specified by the IP Address parameter increments n-1 times.
- If the last octet exceeds 255, it rolls over to 0 and the third octet increments by 1. Note: The Range parameter assigns multiple IP addresses to one virtual server. To generate an array of virtual servers, each of which owns only one IP address, use brackets in the IP Address and Name parameters to specify the range. For example: add lb vserver my_vserver HTTP 192.0.2. 80

serviceType Protocol used by the service (also called the service type).

ngname Nodegroup name to which this lbvsever belongs to

type Type of LB vserver.

state Current LB vserver state.

effectiveState Effective state of the LB vserver , based on the state of backup vservers.

status Current status of the lb vserver. During the initial phase if the configured lb method is not round robin , the vserver will adopt round robin to distribute traffic for a predefined number of requests.

lbrrreason Reason why a vserver is in RR. The following are the reasons: 1 - MEP is DOWN (GSLB) 2 - LB method has changed 3 - Bound service's state changed to UP 4 - A new service is bound 5 - Startup RR factor has changed 6 - LB feature is enabled 7 - Load monitor is not active on a service 8 - Vserver is Enabled 9 - SSL feature is Enabled 10 - All bound services have reached threshold. Using effective state to load balance (GSLB) 11 - Primary state of bound services are not UP. Using effective state to load balance (GSLB) 12 - No LB decision can be made as all bound services have either reached threshold or are not UP (GSLB) 13 - All load monitors are active

cacheType Cache type.

redirect Cache redirect type.

precedence Precedence.

redirectURL The redirect URL.

Authentication Authentication.

authn401 HTTP 401 response based authentication.

authnVsName Name of an authentication virtual server with which to authenticate users.

homePage Home page.

dnsVserverName DNS vserver name.

domain Domain.

policyName Name of the policy bound to the LB vserver.

serviceName Service to bind to the virtual server.

serviceGroupName The service group name bound to the selected load balancing virtual server.

weight Weight to assign to the specified service.

dynamicWeight Dynamic weight

cacheVserver Cache virtual server.

backupVServer Name of the backup virtual server to which to forward requests if the primary virtual server goes DOWN or reaches its spillover threshold.

priority Priority.

cltTimeout The client timeout in seconds.

soMethod The spillover method to be in effect.

soPersistence State of spillover persistence.

soPersistenceTimeOut The maximum time persistence is in effect for a specific client on a spillover vserver.

healthThreshold Threshold in percent of active services below which vserver state is made down.

soThreshold Threshold at which spillover occurs. Specify an integer for the CONNECTION spillover method, a bandwidth value in kilobits per second for the BANDWIDTH method (do not enter the units), or a percentage for the HEALTH method (do not enter the percentage symbol).

soBackupAction Action to be performed if spillover is to take effect, but no backup chain to spillover is usable or exists

lbMethod The load balancing method to be in effect

backupLBMethod Indicates the backup method in case the primary fails

hashLength The hash length.

dataOffset The data offset length for TOKEN load balancing method.

health Health of vserver based on percentage of weights of active svcs/all svcs. This does not consider administratively disabled svcs

dataLength The data length for TOKEN load balancing method.

netmask The netmask of the destination network.

v6netmasklen The netmask of the destination network.

rule Rule type.

resRule Use this parameter to specify the expression to be used in response for RULE persistence type. The string is an in-line expression with a maximum of 1499 characters.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

ruleType Rule type.

groupName LB group to which the lb vserver is to be bound.

m The LB mode.

tosId TOS ID

persistenceType The persistence type for the specified virtual server

timeout The maximum time persistence is in effect for a specific client.

cookieDomain Domain name to be used in the set cookie header in case of cookie persistence.

persistMask The persistence mask for v4 traffic

v6persistmasklen The persistence mask for v6 traffic.

persistenceBackup The maximum time backup persistence is in effect for a specific client.

backupPersistenceTimeout Time period for which backup persistence is in effect.

cacheable The state of caching.

rtspNat Use network address translation (NAT) for RTSP data connections.

sessionless To enable sessionless load balancing, enable this option

trofsPersistence When value is ENABLED, Trofs persistence is honored. When value is DISABLED, Trofs persistence is not honored.

map Map.

connfailover The connection failover mode of the virtual server

redirectPortRewrite Rewrite the port and change the protocol to ensure successful HTTP redirects from services.

downStateFlush Flush all active transactions associated with a virtual server whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions.

disablePrimaryOnDown Tells whether traffic will continue reaching backup vservers even after primary comes UP from DOWN state.

gt2GB Allow for greater than 2 GB transactions on this vserver.

consolidatedLConn Use consolidated stats for LeastConnection.

consolidatedLConnGbl Fetches Global setting.

thresholdValue Tells whether threshold exceeded for this service participating in CUSTOMLB

type The bindpoint to which the policy is bound

invoke Invoke policies bound to a virtual server or policy label.

labelType The invocation type.

labelName Name of the label invoked.

cookieIpPort Encryped Ip address and port of the service that is inserted into the set-cookie http header

cookieName Use this parameter to specify the cookie name for COOKIE peristence type. It specifies the name of cookie with a maximum of 32 characters. If not specified, cookie name is internally generated.

vserverId Vserver Id

version Cookie version

totalServices Total number of services bound to the vserver.

activeServices Total number of active services bound to the vserver.

stateChangeTimeSec Time when last state change happened. Seconds part.

stateChangeTimeSeconds Time when last state change happened. Seconds part.

stateChangeTimemSec Time at which last state change happened. Milliseconds part.

ticksSinceLastStateChange Time in 10 millisecond ticks since the last state change.

hits Number of hits.

piPolicyhits Number of hits.

AuthenticationHost Fully qualified domain name (FQDN) of the authentication virtual server to which the user must be redirected for authentication. Make sure that the Authentication parameter is set to ENABLED.

push Process traffic with the push virtual server that is bound to this load balancing virtual server.

pushVserver Name of the load balancing virtual server, of type PUSH or SSL_PUSH, to which the server pushes updates received on the load balancing virtual server that you are configuring.

pushLabel Expression for extracting a label from the server's response. Can be either an expression or the name of a named expression.

pushMultiClients Allow multiple Web 2.0 connections from the same client to connect to the virtual server and expect updates.

tcpProfileName Name of the TCP profile whose settings are to be applied to the virtual server.

httpProfileName Name of the HTTP profile whose settings are to be applied to the virtual server.

dbProfileName Name of the DB profile whose settings are to be applied to the virtual server.

comment Any comments that you might want to associate with the virtual server.

flag flags policySubType l2Conn Use Layer 2 parameters (channel number, MAC address, and VLAN ID) in addition to the 4-tuple (<source IP>:<source port>::<destination IP>:<destination

port>) that is used to identify a connection. Allows multiple TCP and non-TCP connections with the same 4-tuple to co-exist on the Citrix ADC.

oracleServerVersion Oracle server version

mssqlServerVersion For a load balancing virtual server of type MSSQL, the Microsoft SQL Server version. Set this parameter if you expect some clients to run a version different from the version of the database. This setting provides compatibility between the client-side and server-side connections by ensuring that all communication conforms to the server's version.

mysqlProtocolVersion MySQL protocol version that the virtual server advertises to clients.

mysqlServerVersion MySQL server version string that the virtual server advertises to clients.

mysqlCharacterSet Character set that the virtual server advertises to clients.

mysqlServerCapabilities Server capabilities that the virtual server advertises to clients.

appflowLog Apply AppFlow logging to the virtual server.

netProfile Name of the network profile to associate with the virtual server. If you set this parameter, the virtual server uses only the IP addresses in the network profile as source IP addresses when initiating connections with servers.

isGslb This field is set to true if it is a GSLBVserver.

icmpVsrResponse How the Citrix ADC responds to ping requests received for an IP address that is common to one or more virtual servers. Available settings function as follows:

- If set to PASSIVE on all the virtual servers that share the IP address, the appliance always responds to the ping requests.
- If set to ACTIVE on all the virtual servers that share the IP address, the appliance responds to the ping requests if at least one of the virtual servers is UP. Otherwise, the appliance does not respond.
- If set to ACTIVE on some virtual servers and PASSIVE on the others, the appliance responds if at least one virtual server with the ACTIVE setting is UP. Otherwise, the appliance does not respond. Note: This parameter is available at the virtual server level. A similar parameter, ICMP Response, is available at the IP address level, for IPv4 addresses of type VIP. To set that parameter, use the add ip command in the CLI or the Create IP dialog box in the GUI.

RHIstate Route Health Injection (RHI) functionality of the NetSaler appliance for advertising the route of the VIP address associated with the virtual server. When Vserver RHI Level (RHI) parameter is set to VSVR_CNTRLD, the following are different RHI behaviors for the VIP address on the basis of RHIstate (RHI STATE) settings on the virtual servers associated with the VIP address:

- If you set RHI STATE to PASSIVE on all virtual servers, the Citrix ADC always advertises the route for the VIP address.
- If you set RHI STATE to ACTIVE on all virtual servers, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers is in UP state.
- If you set RHI STATE to ACTIVE on some and PASSIVE on others, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers, whose RHI STATE set to ACTIVE, is in UP state.

newServiceRequest Number of requests, or percentage of the load on existing services, by which to increase the load on a new service at each interval in slow-start mode. A non-zero value indicates that slow-start is applicable. A zero value indicates that the global RR startup parameter is applied. Changing the value to zero will cause services currently in slow start to take the full traffic as determined by the LB method. Subsequently, any new services added will use the global RR factor.

newServiceRequestUnit Units in which to increment load at each interval in slow-start mode.

newServiceRequestIncrementInterval Interval, in seconds, between successive increments in the load on a new service or a service whose state has just changed from DOWN to UP. A value of 0 (zero) specifies manual slow start.

vsvrcfgflags Contains the config info of vserver to be used at validation

vsvrbindsvcip used for showing the ip of bound entities

vsvrbindsvcport used for showing ports of bound entities

preferredLocation Used for displaying the location of bound services.

persistAVPno Persist AVP number for Diameter Persistency. In case this AVP is not defined in Base RFC 3588 and it is nested inside a Grouped AVP, define a sequence of AVP numbers (max 3) in order of parent to child. So say persist AVP number X is nested inside AVP Y which is nested in Z, then define the list as Z Y X

state State of the load balancing virtual server.

skippersistency This argument decides the behavior incase the service which is selected from an existing persistence session has reached threshold.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

minAutoscaleMembers Minimum number of members expected to be present when vserver is used in Autoscale.

maxAutoscaleMembers Maximum number of members expected to be present when vserver is used in Autoscale.

authnProfile Name of the authentication profile to be used when authentication is turned on.

macmodeRetainvlan This option is used to retain vlan information of incoming packet when macmode is enabled

dbsLb Enable database specific load balancing for MySQL and MSSQL service types.

dns64 This argument is for enabling/disabling the dns64 on lbvserver

bypassAAAA If this option is enabled while resolving DNS64 query AAAA queries are not sent to back end dns server

RecursionAvailable When set to YES, this option causes the DNS replies from this vserver to have the RA bit turned on. Typically one would set this option to YES, when the vserver is load balancing a set of DNS servers thatsupport recursive queries.

processLocal By turning on this option packets destined to a vserver in a cluster will not under go any steering. Turn this option for single packet request response mode or when the upstream device is performing a proper RSS for connection based distribution.

vsvrdynconnsothreshold Spillover threshold for dynamic connection

backupVserverStatus Staus of BackUp Vserver .

dnsProfileName Name of the DNS profile to be associated with the VServer. DNS profile properties will be applied to the transactions processed by a VServer. This parameter is valid only for DNS and DNS-TCP VServers.

lbprofilename Name of the LB profile which is associated to the vserver

redirectFromPort Port number for the virtual server, from which we absorb the traffic for http redirect

httpsRedirectUrl URL to which all HTTP traffic received on the port specified in the -redirectFromPort parameter is redirected.

retainConnectionsOnCluster This option enables you to retain existing connections on a node joining a Cluster system or when a node is being configured for passive timeout. By default, this option is disabled.

analyticsProfile Name of the analytics profile bound to the LB vserver.

noDefaultBindings to determine if the configuration will have default ssl CIPHER and ECC curve bindings

adfsProxyProfile Name of the adfsProxy profile to be used to support ADFSPIP protocol for ADFS servers.

tcpProbePort Port number for external TCP probe. NetScaler provides support for external TCP health check of the vserver status over the selected port. This option is only supported for vservers assigned with an IPAddress or ipset.

isFirstGracefulMember Used for display purpose to find whether this is first binding of service group.

quicBridgeProfilename Name of the QUIC Bridge profile whose settings are to be applied to the virtual server.

probeProtocol Citrix ADC provides support for external health check of the vserver status. Select HTTP or TCP probes for healthcheck

probePort Citrix ADC provides support for external health check of the vserver status. Select port for HTTP/TCP monitring

probeSuccessResponseCode HTTP code to return in SUCCESS case.

quicProfileName Name of QUIC profile which will be attached to the VServer.

order Order number to be assigned to the service when it is bound to the lb vserver.

order Order in string form assigned to the service when it is bound to the lb vserver.

toggleorder Configure this option to toggle order preference

orderthreshold This option is used to to specify the threshold of minimum number of services to be UP in an order, for it to be considered in Lb decision.

CurrentActiveOrder current order that takes the traffic in case service or servicegroup is bound with order

devno count

rename lb vserver

Renames a load balancing virtual server.

Synopsis

rename lb vserver <name>@ <newName>@

Arguments

name Existing name of the virtual server.

newName New name for the virtual server.

Example

rename lb vserver http_vsvr http_vsvr_new

rm lb vserver

Removes a virtual server from the Citrix ADC.

Synopsis

rm lb vserver <name>@ ...

Arguments

name Name of the virtual server.

Example

rm vserver lb_vip To remove multiple vservers use the following command: rm vserver lb_vip

unset lb vserver

Removes the specified parameter settings from the virtual server..Refer to the set lb vserver command for meanings of the arguments.

Synopsis

unset lb vserver <name>@ [<serviceName>@]

Example

unset lb vserver lb_vip -backupVServer To unset the backup virtual server for multiple vservers use the following command: unset lb vserver lb_vip -backupVServer

stat lb vserver

Displays the statistical data collected for a load balancing virtual server.

Synopsis

stat lb vserver [-sortBy (Hits | CPU-PM)]

Arguments

name Name of the virtual server. If no name is provided, statistical data of all configured virtual servers is displayed.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

sortBy use this argument to sort by specific key

Possible values: Hits, CPU-PM

sortOrder use this argument to specify sort order

Possible values: ascending, descending Default value: SORT_DESCENDING

Output

count devno stateflag

Counters

Average client TTLB (cltTTLB) Average TTLB between the client and the server. TTLB is the time interval between sending the request packet to a service and receiving the ACK for response from client.

Apdex for client response times. (cltResponseTimeApdex) Vserver APDEX index based on client response times.

Requests in vserver's surgeQ (vSurgeQ) Number of requests waiting on this vserver.

Current Client Est connections (ClntEstConn) Number of client connections in ESTABLISHED state.

Number of Bytes processed by ADS Service Total IP payload sent and received

total INACTIVE services (inactSvcs) number of INACTIVE services bound to a vserver

Vserver Health (Health) Health of the vserver. This gives percentage of UP services bound to this vserver.

Vserver IP address (vsvrIP) IP address of the vserver

Port (port) The port on which the service is running.

Vserver protocol (Protocol) Protocol associated with the vserver

State Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)

total ACTIVE services (actSvcs) number of ACTIVE services bound to a vserver

CPU Use(per-mille) (CPU-PM) Vserver CPU usage in per-mille(parts per thousand)

Vserver hits (Hits) Total vserver hits

Requests (Req) Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Responses (Rsp) Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Request bytes (Reqb) Total number of request bytes received on this service or virtual server.

Response bytes (Rspb) Number of response bytes received by this service or virtual server.

Http2 Requests (H2Req) Total number of Http2 requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Http2 Responses (H2Rsp) Number of Http2 responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Total Packets rcvd (PktRx) Total number of packets received by this service or virtual server.

Total Packets sent (PktTx) Total number of packets sent.

Current client connections (ClntConn) Number of current client connections.

Current server connections (SvrConn) Number of current connections to the actual servers behind the virtual server.

Current Persistence Sessions (PersistenceSessions) current vserver owned persistence sessions

Current Backup Persistence Sessions (BackupPersistenceSessions) current vserver owned backup persistence sessions

Requests in surge queue (SurgeQ) Number of requests in the surge queue.

Requests in service's surgeQs (SvcSurgeQ) Total number of requests in the surge queues of all the services bound to this LB-vserver.

Spill Over Threshold (SOThresh) Spill Over Threshold set on the VServer.

Spill Over Hits (NumSo) Number of times vserver experienced spill over.

Labeled Connection (LblConn) Number of Labeled connection on this vserver

Push Labeled Connection (PushLbl) Number of labels for this push vserver.

Deferred Request (DefReq) Number of deferred request on this vserver

Invalid Request/Response (IvldReqRsp) Number invalid requests/responses on this vserver

Invalid Request/Response Dropped (lvldReqRspDrp) Number invalid requests/responses dropped on this vserver

Vserver Down Backup Hits (VserverDownBackupHits) Number of times traffic was diverted to backup vserver since primary vserver was DOWN.

Current Multipath TCP sessions (MptcpSess) Current Multipath TCP sessions

Current Multipath TCP subflows (subflowConn) Current Multipath TCP subflows

No of TCPConn ReasmQ 75% reached (ReassQ75) Total no of connections with 75% TCP reassembly queue

No of TCPConn ReasmQ Flushed (ReassQFlush) Total no of connections incurred TCP reassembly queue flush

No of Server Busy Error (totalSvrBusyErr) Total no of server busy error

Request retry count (RequestRetryCount) Number of times request has been retried due to server failure.

Maximum retry count exceeded (RequestRetryCountExceeded) Number of times Maximum retry count threshold is exceeded and error returned to client.

No of http max header size packet parsing failures (httpMaxHdrSzPkts) Number of http max header size packet parsing failures

Number of HTTP requests exceeding max header field length (httpMaxHdrFldLenPkts) Number of HTTP requests exceeding max header field length

max ooo packets threshold hits (tcpMaxoooPkts) No of times max out of order packets reached

Total transactions for Client TTLB (totCltTTLBTransactions) Total transactions where client TTLB is calculated.

Tolerating TTLB Transactions (toleratingTTLBTransactions) Tolerable transactions based on APDEX threshold (>T && <4T).

Frustrating TTLB Transactions (frustratingTTLBTransactions) Frustrating transactions based on APDEX threshold (>4T).

Current Server Est connections (SvrEstConn) Number of server connections in ESTABLISHED state.

Related Commands

- stat lb policylabel

lb-wlm

The following operations can be performed on "lb-wlm":

set| unset| unbind| bind| add| rm| show|

set lb wlm

set Work Load Manager attributes NOTE: This command is deprecated.

Synopsis

Arguments

wlmName The name of the work load manager.

KATimeout The idle time period after which Citrix ADC would probe the WLM. The value ranges from 1 to 1440 minutes. Default value: 2 Maximum value: 1440

Example

set lb wlm ibm_wlm -ka_timeout 6

unset lb wlm

Use this command to remove lb wlm settings.Refer to the set lb wlm command for meanings of the arguments.NOTE: This command is deprecated.

Synopsis

unbind lb wlm

Unbind a vserver from Work Load Manager. NOTE: This command is deprecated.WLM feature has been deprecated from Kos onwards as classic build is not supported.

Synopsis

Arguments

wlmName The name of the Work Load Manager.

vServerName Name of the virtual server which is to be unbound from the WLM.

Example

unbind lb wlm ibm_wlm http_vip To unbind multiple vservers from Work Load Manager use the following command: unbind lb wlm ibm_wlm http_vip

bind lb wlm

Bind a vserver to Work Load Manager. NOTE: This command is deprecated.WLM feature has been deprecated from Kos onwards as classic build is not supported.

Synopsis

Arguments

wlmName The name of the Work Load Manager.

vServerName Name of the virtual server which is to be bound to the WLM.

Example

bind lb wlm ibm_wlm http_vip To bind multiple vservers to workload manager use the following command: bind lb wlm ibm_wlm http_vip

add lb wlm

Add a Work Load Manager. NOTE: This command is deprecated.WLM feature has been deprecated from Kos onwards as classic build is not supported.

Synopsis

Arguments

wlmName The name of the Work Load Manager.

IPAddress The IP address of the WLM.

port The port of the WLM.

LBUID The LBUID for the Load Balancer to communicate to the Work Load Manager.

KATimeout The idle time period after which Citrix ADC would probe the WLM. The value ranges from 1 to 1440 minutes. Default value: 2 Maximum value: 1440

Example

add lb wlm ibm_wlm 10.102.1.10 3060

rm lb wlm

Removes a Work Load Manager. NOTE: This command is deprecated.WLM feature has been deprecated from Kos onwards as classic build is not supported.

Synopsis

Arguments

wlmName The name of the Work Load Manager to be removed.

Example

rm lb wlm ibm_wlm

show lb wlm

show Work Load Manager details NOTE: This command is deprecated.WLM feature has been deprecated from Kos onwards as classic build is not supported.

Synopsis

Arguments

wlmName The name of the work load manager.

Output

IPAddress The IP address of the WLM.

port A port number for the virtual server.

stateflag secure Use this parameter to enable secure mode of communication with WLM.

KATimeout The idle time period after which Citrix ADC would probe the WLM. The value ranges from 1 to 1440 minutes.

LBUID The LBUID for the Load Balancer to communicate to the Work Load Manager.

state State of the WLM.

vServerName Name of the virtual server which is to be bound to the WLM.

devno count

Example

show lb wlm ibm_wlm

lldp

Lldp

The entities on which you can perform NetScaler CLI operations:

- lldp
- lldp-neighbors
- lldp-param
- lldp-stats

lldp-neighbors

The following operations can be performed on "lldp-neighbors":

clear| show|

clear lldp neighbors

Removes LLDP neighbor info of interfaces

Synopsis

clear lldp neighbors

show lldp neighbors

Display Neighbor information per interface

Synopsis

show lldp neighbors

Arguments

ifnum Interface Name

Output

chassisIdSubtype Chassis id sub type

chassisId Chassis Id

portIdSubtype Port id subtype

portId Port Id

TTL Time to Live

portDescription Port Description

sys System Name

sysDesc System Description

mgmtAddressSubtype Management Address Type

mgmtAddress Management Address

iftype Interface subtype

ifNumber Interface Number

vlan vlan name

vlanId Vlan Id

portProtoSupported Flag to show Port Protocol Support

portProtoEnabled Flag to show Port Protocol support enabled

portProtoId Port Protocol ID

portVlanId Port Vlan Id

protocolId port vlan id name

linkAggrCapable Is neighbor Link Aggregation Capable

LinkAggrEnabled Is link aggregation Enabled

linkAggrId Link Aggregation Id

flag sysCapabilities Temp System Capabilities

sysCapabilities Acronyms for remote system capabilities: OT : Other. RE : Repeater(IETF RFC 2108). BR : MAC Bridge(IEEE Std 802.1D). WL : WLAN Access Point(IEEE Std 802.11 MIB). RO : ROuter(IETF RFC 1812). TE : Telephone(IETF RFC 4293). DO : DOCSIS cable device(IETF RFC

4639 and IETF RFC 4546). ST : STation only(IETF RFC 4293). CV : C-VLAN component of a VLAN Bridge(IEEE Std 802.1Q). SV : S-VLAN component of a VLAN Bridge(IEEE Std 802.1Q). MR : Two port MAC Relay(IEEE Std 802.1Q).

sysCapEnabled Temp system enabled capabilities

sysCapEnabled Acronyms for remote system enabled capabilities: OT : Other. RE : Repeater(IETF RFC 2108). BR : MAC Bridge(IEEE Std 802.1D). WL : WLAN Access Point(IEEE Std 802.11 MIB). RO : ROuter(IETF RFC 1812). TE : Telephone(IETF RFC 4293). DO : DOCSIS cable device(IETF RFC 4639 and IETF RFC 4546). ST : STation only(IETF RFC 4293). CV : C-VLAN component of a VLAN Bridge(IEEE Std 802.1Q). SV : S-VLAN component of a VLAN Bridge(IEEE Std 802.1Q). MR : Two port MAC Relay(IEEE Std 802.1Q).

autonegSupport MAC/PHY autonegotiation support

autonegEnabled MAC/PHY autonegotiation enabled

autonegAdvertised MAC/PHY autonegotiation advetised

autonegAdvertised MAC/PHY autonegotiation advetised

autonegMAUType MAC/PHY Medium Attachment Unit (MAU) type of the port. Description listed below: AUI - no internal MAU, view from AUI 10Base5 - thick coax MAU Foirl - FOIRL MAU 10Base2 - thin coax MAU 10BaseT - UTP MAU 10BaseFP - passive fiber MAU 10BaseFB - sync fiber MAU 10BaseFL - async fiber MAU 10Broad36 - broadband DTE MAU 10BaseTHD - UTP MAU, half duplex mode 10BaseTFD - UTP MAU, full duplex mode 10BaseFLHD - async fiber MAU, half duplex mode 10BaseFLDF - async fiber MAU, full duplex mode 10BaseT4 - 4 pair category 3 UTP 100BaseTXHD - 2 pair category 5 UTP, half duplex mode 100BaseTXFD - 2 pair category 5 UTP, full duplex mode 100BaseFXHD - X fiber over PMT, half duplex mode 100BaseFXFD - X fiber over PMT, full duplex mode 100BaseT2HD - 2 pair category 3 UTP, half duplex mode 100BaseT2DF - 2 pair category 3 UTP, full duplex mode 1000BaseXHD - PCS/PMA, unknown PMD, half duplex mode 1000BaseXFD - PCS/PMA, unknown PMD, full duplex mode 1000BaseLXHD - Fiber over long-wavelength laser, half duplex mode 1000BaseLXFD - Fiber over long-wavelength laser, full duplex mode 1000BaseSXHD - Fiber over short-wavelength laser, half duplex mode 1000BaseSXFD - Fiber over short-wavelength laser, full duplex mode 1000BaseCXHD - Copper over 150-Ohm balanced cable, half duplex mode 1000BaseCXFD - Copper over 150-Ohm balanced cable, full duplex mode 1000BaseTHD - Four-pair Category 5 UTP, half duplex mode 1000BaseTFD - Four-pair Category 5 UTP, full duplex mode 10GigBaseX - X PCS/PMA, unknown PMD 10GigBaseLX4 - X fiber over WWDM optics 10GigBaseR - R PCS/PMA, unknown PMD 10GigBaseER - R fiber over 1550 nm optics 10GigBaseLR - R fiber over

1310 nm optics 10GigBaseSR - R fiber over 850 nm optics 10GigBaseW - W PCS/PMA, unknown PMD 10GigBaseEW - W fiber over 1550 nm optics 10GigBaseLW - W fiber over 1310 nm optics 10GigBaseSW - W fiber over 850 nm optics

mtu MTU of Remote Device

devno count stateflag

lldp-param

The following operations can be performed on "lldp-param":

show| set| unset|

show lldp param

Display the global LLDP params

Synopsis

show lldp param

Arguments

Output

holdtimeTxMult A multiplier for calculating the duration for which the receiving device stores the LLDP information in its database before discarding or removing it. The duration is calculated as the holdtimeTxMult (Holdtime Multiplier) parameter value multiplied by the timer (Timer) parameter value.

timer Interval, in seconds, between LLDP packet data units (LLDPDUs). that the Citrix ADC sends to a directly connected device.

Mode Global mode of Link Layer Discovery Protocol (LLDP) on the Citrix ADC. The resultant LLDP mode of an interface depends on the LLDP mode configured at the global and the interface levels.

Example

show lldpparam

set lldp param

Sets the global Link Layer Discovery Protocol (LLDP) parameters such as LLDP Timer, Hold Time Multiplier, and LLDP mode.

Synopsis

set lldp param

Arguments

holdtimeTxMult A multiplier for calculating the duration for which the receiving device stores the LLDP information in its database before discarding or removing it. The duration is calculated as the holdtimeTxMult (Holdtime Multiplier) parameter value multiplied by the timer (Timer) parameter value. Default value: 4 Minimum value: 1 Maximum value: 20

timer Interval, in seconds, between LLDP packet data units (LLDPDUs). that the Citrix ADC sends to a directly connected device. Default value: 30 Minimum value: 1 Maximum value: 3000

Mode Global mode of Link Layer Discovery Protocol (LLDP) on the Citrix ADC. The resultant LLDP mode of an interface depends on the LLDP mode configured at the global and the interface levels.

Possible values: NONE, TRANSMITTER, RECEIVER, TRANSCEIVER

Example

set lldpparam -mode RECEIVER

unset lldp param

Use this command to remove lldp param settings.Refer to the set lldp param command for meanings of the arguments.

Synopsis

unset lldp param

lldp-stats

The following operations can be performed on "lldp-stats":

show lldp stats

show lldp stats is an alias for stat lldp Display LLDP stats

Synopsis

show lldp stats - alias for 'stat lldp'

lldp

The following operations can be performed on "lldp":

stat lldp

DIsplay lldp statistics.

Synopsis

stat lldp

Arguments

ifnum LLDP Statistics per interfaces

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

LLDP received Packets (RxPkts) Total LLDP Packets received.

LLDP bytes received (RxBytes) Total LLDP bytes received

LLDP packets transmitted (TxPkts) Total LLDP Packets transmitted

LLDP bytes transmitted (TxBytes) Total LLDP bytes transmitted.

Errors in LLDP Packets (RxErrPkts) Total errors in LLDP packets.

Discarded LLDP Packets (DiscardPkts) Total discarded LLDP packets.

TLVs not Recognised (TlvNotRecognised) Total TLVs not Recognised.

lsn

lsn-appsattributes

The following operations can be performed on "lsn-appsattributes":

set| add| show| rm| unset|

set lsn appsattributes

Set LSN Application Port ATTRIBUTES.

Synopsis

set lsn appsattributes <name> -sessiontimeout <secs>

Arguments

name Name for the LSN Application Port ATTRIBUTES. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN application profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn application profile1" or 'lsn application profile1').

sessiontimeout Timeout, in seconds, for an idle LSN session. If an LSN session is idle for a time that exceeds this value, the Citrix ADC removes the session.This timeout does not apply for a TCP LSN session when a FIN or RST message is received from either of the endpoints. Default value: 30 Minimum value: 5 Maximum value: 600

Example

Set lsn APPSATTRIBUTES s1 -timeout 40

add lsn appsattributes

Add LSN Application Port ATTRIBUTES.

Synopsis

add lsn appsattributes <name> <transportprotocol> [-port <port>]

Arguments

name Name for the LSN Application Port ATTRIBUTES. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN application profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn application profile1" or 'lsn application profile1').

transportprotocol Name of the protocol(TCP,UDP) for which the parameters of this LSN application port ATTRIBUTES applies

Possible values: TCP, UDP, ICMP

port This is used for Displaying Port/Port range in CLI/Nitro.Lowport, Highport values are populated and used for displaying.Port numbers or range of port numbers to match against the destination port of the incoming packet from a subscriber. When the destination port is matched, the LSN application profile is applied for the LSN session. Separate a range of ports with a hyphen. For example, 40-90. Minimum value: 1

sessiontimeout Timeout, in seconds, for an idle LSN session. If an LSN session is idle for a time that exceeds this value, the Citrix ADC removes the session.This timeout does not apply for a TCP LSN session when a FIN or RST message is received from either of the endpoints. Default value: 30 Minimum value: 5 Maximum value: 600

Example

add lsn appsattributes s1 TCP -port 53 -sesstimeout 30

show lsn appsattributes

Display LSN Application Port ATTRIBUTES.

Synopsis

show lsn appsattributes

Arguments

name Name for the LSN Application Port ATTRIBUTES. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN application profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn application profile1" or 'lsn application profile1').

Output

transportprotocol Name of the protocol(TCP,UDP) for which the parameters of this LSN application port ATTRIBUTES applies

sessiontimeout Timeout, in seconds, for an idle LSN session. If an LSN session is idle for a time that exceeds this value, the Citrix ADC removes the session.This timeout does not apply for a TCP LSN session when a FIN or RST message is received from either of the endpoints.

port This is used for Displaying Port/Port range in CLI/Nitro.Lowport, Highport values are populated and used for displaying.Port numbers or range of port numbers to match against the destination port of the incoming packet from a subscriber. When the destination port is matched, the LSN application profile is applied for the LSN session. Separate a range of ports with a hyphen. For example, 40-90.

firstport Indicates first parameter of Port-range. Lowport and Highport will be same for single port value.Port numbers or range of port numbers to match against the destination port of the incoming packet from a subscriber. When the destination port is matched, the LSN application profile is applied for the LSN session. Separate a range of ports with a hyphen. For example, 40-90.

lastport Indicates second parameter of Port-range.Low port and Highport will be same for single port value.Port numbers or range of port numbers to match against the destination port of the incoming packet from a subscriber. When the destination port is matched, the LSN application profile is applied for the LSN session. Separate a range of ports with a hyphen. For example, 40-90.

devno count stateflag

Example

show lsn APPSATTRIBUTES s1

rm lsn appsattributes

Remove LSN Application Port ATTRIBUTES.

Synopsis

rm lsn appsattributes <name>

Arguments

name Name for the LSN Application Port ATTRIBUTES. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN application profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn application profile1" or 'lsn application profile1').

Example

rm lsn APPSATTRIBUTES s1

unset lsn appsattributes

Use this command to remove lsn appsattributes settings.Refer to the set lsn appsattributes command for meanings of the arguments.

Synopsis

unset lsn appsattributes <name> -sessiontimeout

lsn-appsprofile

The following operations can be performed on "lsn-appsprofile":

unbind| bind| rm| show| set| unset| add|

unbind lsn appsprofile

Unbind LSN Application Profile.

Synopsis

unbind lsn appsprofile <appsprofilename> (<lsnport> | -appsattributesname <string>)

Arguments

appsprofilename Name for the LSN application profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN application profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn application profile1" or 'lsn application profile1').

lsnport Port numbers or range of port numbers to match against the destination port of the incoming packet from a subscriber. When the destination port is matched, the LSN application profile is applied for the LSN session. Separate a range of ports with a hyphen. For example, 40-90. Minimum value: 1

appsattributesname Name of the LSN application port ATTRIBUTES command to bind to the specified LSN Appsprofile. Properties of the Appsprofile will be applicable to this APPSATTRIBUTES

Example

unbind lsn appsprofile profile1 80-100

bind lsn appsprofile

Bind LSN Application Profile.

Synopsis

bind lsn appsprofile <appsprofilename> (<lsnport> | -appsattributesname <string>)

Arguments

appsprofilename Name for the LSN application profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN application profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn application profile1" or 'lsn application profile1').

lsnport Port numbers or range of port numbers to match against the destination port of the incoming packet from a subscriber. When the destination port is matched, the LSN application

profile is applied for the LSN session. Separate a range of ports with a hyphen. For example, 40-90. Minimum value: 1

appsattributesname Name of the LSN application port ATTRIBUTES command to bind to the specified LSN Appsprofile. Properties of the Appsprofile will be applicable to this APPSATTRIBUTES

Example

bind lsn appsprofile profile1 80-100

rm lsn appsprofile

Remove LSN Application Profile.

Synopsis

rm lsn appsprofile <appsprofilename>

Arguments

appsprofilename Name for the LSN application profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN application profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn application profile1" or 'lsn application profile1').

Example

rm lsn appsprofile profile1

show lsn appsprofile

Display LSN Application Profile.

Synopsis

show lsn appsprofile

Arguments

appsprofilename Name for the LSN application profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the

LSN application profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn application profile1" or 'lsn application profile1').

Output

lsnport Port numbers or range of port numbers to match against the destination port of the incoming packet from a subscriber. When the destination port is matched, the LSN application profile is applied for the LSN session. Separate a range of ports with a hyphen. For example, 40-90.

transportprotocol Name of the protocol for which the parameters of this LSN application profile applies.

ippooling NAT IP address allocation options for sessions associated with the same subscriber.

Available options function as follows:

- Paired - The Citrix ADC allocates the same NAT IP address for all sessions associated with the same subscriber. When all the ports of a NAT IP address are used in LSN sessions (for same or multiple subscribers), the Citrix ADC ADC drops any new connection from the subscriber.
- Random - The Citrix ADC allocates random NAT IP addresses, from the pool, for different sessions associated with the same subscriber.

This parameter is applicable to dynamic NAT allocation only.

mapping Type of LSN mapping to apply to subsequent packets originating from the same subscriber IP address and port.

Consider an example of an LSN mapping that includes the mapping of the subscriber IP:port (X:x), NAT IP:port (N:n), and external host IP:port (Y:y).

Available options function as follows:

- ENDPOINT-INDEPENDENT - Reuse the LSN mapping for subsequent packets sent from the same subscriber IP address and port (X:x) to any external IP address and port.
- ADDRESS-DEPENDENT - Reuse the LSN mapping for subsequent packets sent from the same subscriber IP address and port (X:x) to the same external IP address (Y), regardless of the external port.

- ADDRESS-PORT-DEPENDENT - Reuse the LSN mapping for subsequent packets sent from the same internal IP address and port (X:x) to the same external IP address and port (Y:y) while the mapping is still active.

filtering Type of filter to apply to packets originating from external hosts.

Consider an example of an LSN mapping that includes the mapping of subscriber IP:port (X:x), NAT IP:port (N:n), and external host IP:port (Y:y).

Available options function as follows:

- ENDPOINT INDEPENDENT - Filters out only packets not destined to the subscriber IP address and port X:x, regardless of the external host IP address and port source (Z:z). The Citrix ADC forwards any packets destined to X:x. In other words, sending packets from the subscriber to any external IP address is sufficient to allow packets from any external hosts to the subscriber.
- ADDRESS DEPENDENT - Filters out packets not destined to subscriber IP address and port X:x. In addition, the ADC filters out packets from Y:y destined for the subscriber (X:x) if the client has not previously sent packets to Y:anyport (external port independent). In other words, receiving packets from a specific external host requires that the subscriber first send packets to that specific external host's IP address.
- ADDRESS PORT DEPENDENT (the default) - Filters out packets not destined to subscriber IP address and port (X:x). In addition, the Citrix ADC filters out packets from Y:y destined for the subscriber (X:x) if the subscriber has not previously sent packets to Y:y. In other words, receiving packets from a specific external host requires that the subscriber first send packets first to that external IP address and port.

tcpproxy Enable TCP proxy, which enables the Citrix ADC to optimize the TCP traffic by using Layer 4 features.

td ID of the traffic domain through which the Citrix ADC sends the outbound traffic after performing LSN.

If you do not specify an ID, the ADC sends the outbound traffic through the default traffic domain, which has an ID of 0.

l2info Enable l2info by creating natpcbs for LSN, which enables the Citrix ADC to use L2CONN/ MBF with LSN.

firstport Port numbers or range of port numbers to match against the destination port of the incoming packet from a subscriber. When the destination port is matched, the LSN application

profile is applied for the LSN session. Separate a range of ports with a hyphen. For example, 40-90.

lastport Port numbers or range of port numbers to match against the destination port of the incoming packet from a subscriber. When the destination port is matched, the LSN application profile is applied for the LSN session. Separate a range of ports with a hyphen. For example, 40-90.

appsattributesname Name of the LSN application port ATTRIBUTES command to bind to the specified LSN Appsprofile. Properties of the Appsprofile will be applicable to this APPSATTRIBUTES

devno count stateflag

Example

show lsn appsprofile profile1

set lsn appsprofile

Set LSN Application Profile.

Synopsis

set lsn appsprofile <appsprofilename>

Arguments

appsprofilename Name for the LSN application profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN application profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn application profile1" or 'lsn application profile1').

ippooling NAT IP address allocation options for sessions associated with the same subscriber.

Available options function as follows:

- Paired - The Citrix ADC allocates the same NAT IP address for all sessions associated with the same subscriber. When all the ports of a NAT IP address are used in LSN sessions (for same or multiple subscribers), the Citrix ADC ADC drops any new connection from the subscriber.

- Random - The Citrix ADC allocates random NAT IP addresses, from the pool, for different sessions associated with the same subscriber.

This parameter is applicable to dynamic NAT allocation only.

Possible values: PAIRED, RANDOM Default value: RANDOM

mapping Type of LSN mapping to apply to subsequent packets originating from the same subscriber IP address and port.

Consider an example of an LSN mapping that includes the mapping of the subscriber IP:port (X:x), NAT IP:port (N:n), and external host IP:port (Y:y).

Available options function as follows:

- ENDPOINT-INDEPENDENT - Reuse the LSN mapping for subsequent packets sent from the same subscriber IP address and port (X:x) to any external IP address and port.
- ADDRESS-DEPENDENT - Reuse the LSN mapping for subsequent packets sent from the same subscriber IP address and port (X:x) to the same external IP address (Y), regardless of the external port.
- ADDRESS-PORT-DEPENDENT - Reuse the LSN mapping for subsequent packets sent from the same internal IP address and port (X:x) to the same external IP address and port (Y:y) while the mapping is still active.

Possible values: ENDPOINT-INDEPENDENT, ADDRESS-DEPENDENT, ADDRESS-PORT-DEPENDENT Default value: ADDRESS-PORT-DEPENDENT

filtering Type of filter to apply to packets originating from external hosts.

Consider an example of an LSN mapping that includes the mapping of subscriber IP:port (X:x), NAT IP:port (N:n), and external host IP:port (Y:y).

Available options function as follows:

- ENDPOINT INDEPENDENT - Filters out only packets not destined to the subscriber IP address and port X:x, regardless of the external host IP address and port source (Z:z). The Citrix ADC forwards any packets destined to X:x. In other words, sending packets from the subscriber to any external IP address is sufficient to allow packets from any external hosts to the subscriber.
- ADDRESS DEPENDENT - Filters out packets not destined to subscriber IP address and port X:x. In addition, the ADC filters out packets from Y:y destined for the subscriber (X:x) if the client has not previously sent packets to Y:anyport (external port independent). In other words,

receiving packets from a specific external host requires that the subscriber first send packets to that specific external host's IP address.

- ADDRESS PORT DEPENDENT (the default) - Filters out packets not destined to subscriber IP address and port (X:x). In addition, the Citrix ADC filters out packets from Y:y destined for the subscriber (X:x) if the subscriber has not previously sent packets to Y:y. In other words, receiving packets from a specific external host requires that the subscriber first send packets first to that external IP address and port.

Possible values: ENDPOINT-INDEPENDENT, ADDRESS-DEPENDENT, ADDRESS-PORT-DEPENDENT Default value: ADDRESS-PORT-DEPENDENT

tcpproxy Enable TCP proxy, which enables the Citrix ADC to optimize the TCP traffic by using Layer 4 features.

Possible values: ENABLED, DISABLED Default value: DISABLED

td ID of the traffic domain through which the Citrix ADC sends the outbound traffic after performing LSN.

If you do not specify an ID, the ADC sends the outbound traffic through the default traffic domain, which has an ID of 0. Default value: 4095 Minimum value: 0

l2info Enable l2info by creating natpcbs for LSN, which enables the Citrix ADC to use L2CONN/MBF with LSN.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

Set lsn appsprofile profile1 -mapping ENDPOINT-INDEPENDENT

unset lsn appsprofile

Use this command to remove lsn appsprofile settings.Refer to the set lsn appsprofile command for meanings of the arguments.

Synopsis

unset lsn appsprofile <appsprofilename>

add lsn appsprofile

Add LSN Application Profile.

Synopsis

add lsn appsprofile <appsprofilename> <transportprotocol>

Arguments

appsprofilename Name for the LSN application profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN application profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn application profile1" or 'lsn application profile1').

transportprotocol Name of the protocol for which the parameters of this LSN application profile applies.

Possible values: TCP, UDP, ICMP

ippooling NAT IP address allocation options for sessions associated with the same subscriber.

Available options function as follows:

- Paired - The Citrix ADC allocates the same NAT IP address for all sessions associated with the same subscriber. When all the ports of a NAT IP address are used in LSN sessions (for same or multiple subscribers), the Citrix ADC ADC drops any new connection from the subscriber.
- Random - The Citrix ADC allocates random NAT IP addresses, from the pool, for different sessions associated with the same subscriber.

This parameter is applicable to dynamic NAT allocation only.

Possible values: PAIRED, RANDOM Default value: RANDOM

mapping Type of LSN mapping to apply to subsequent packets originating from the same subscriber IP address and port.

Consider an example of an LSN mapping that includes the mapping of the subscriber IP:port (X:x), NAT IP:port (N:n), and external host IP:port (Y:y).

Available options function as follows:

- ENDPOINT-INDEPENDENT - Reuse the LSN mapping for subsequent packets sent from the same subscriber IP address and port (X:x) to any external IP address and port.

- ADDRESS-DEPENDENT - Reuse the LSN mapping for subsequent packets sent from the same subscriber IP address and port (X:x) to the same external IP address (Y), regardless of the external port.
- ADDRESS-PORT-DEPENDENT - Reuse the LSN mapping for subsequent packets sent from the same internal IP address and port (X:x) to the same external IP address and port (Y:y) while the mapping is still active.

Possible values: ENDPOINT-INDEPENDENT, ADDRESS-DEPENDENT, ADDRESS-PORT-DEPENDENT Default value: ADDRESS-PORT-DEPENDENT

filtering Type of filter to apply to packets originating from external hosts.

Consider an example of an LSN mapping that includes the mapping of subscriber IP:port (X:x), NAT IP:port (N:n), and external host IP:port (Y:y).

Available options function as follows:

- ENDPOINT INDEPENDENT - Filters out only packets not destined to the subscriber IP address and port X:x, regardless of the external host IP address and port source (Z:z). The Citrix ADC forwards any packets destined to X:x. In other words, sending packets from the subscriber to any external IP address is sufficient to allow packets from any external hosts to the subscriber.
- ADDRESS DEPENDENT - Filters out packets not destined to subscriber IP address and port X:x. In addition, the ADC filters out packets from Y:y destined for the subscriber (X:x) if the client has not previously sent packets to Y:anyport (external port independent). In other words, receiving packets from a specific external host requires that the subscriber first send packets to that specific external host's IP address.
- ADDRESS PORT DEPENDENT (the default) - Filters out packets not destined to subscriber IP address and port (X:x). In addition, the Citrix ADC filters out packets from Y:y destined for the subscriber (X:x) if the subscriber has not previously sent packets to Y:y. In other words, receiving packets from a specific external host requires that the subscriber first send packets first to that external IP address and port.

Possible values: ENDPOINT-INDEPENDENT, ADDRESS-DEPENDENT, ADDRESS-PORT-DEPENDENT Default value: ADDRESS-PORT-DEPENDENT

tcpproxy Enable TCP proxy, which enables the Citrix ADC to optimize the TCP traffic by using Layer 4 features.

Possible values: ENABLED, DISABLED Default value: DISABLED

td ID of the traffic domain through which the Citrix ADC sends the outbound traffic after performing LSN.

If you do not specify an ID, the ADC sends the outbound traffic through the default traffic domain, which has an ID of 0. Default value: 4095 Minimum value: 0

l2info Enable l2info by creating natpcbs for LSN, which enables the Citrix ADC to use L2CONN/ MBF with LSN.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

add lsn appsprofile profile1 TCP -mapping ENDPOINT-INDEPENDENT

lsn-client

The following operations can be performed on "lsn-client":

show| unbind| rm| bind| add|

show lsn client

Display LSN Client.

Synopsis

show lsn client

Arguments

clientname Name for the LSN client entity. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN client is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn client1" or 'lsn client1').

Output

network IPv4 address(es) of the LSN subscriber(s) or subscriber network(s) on whose traffic you want the Citrix ADC to perform Large Scale NAT.

netmask Subnet mask for the IPv4 address specified in the Network parameter.

td ID of the traffic domain on which this subscriber or the subscriber network (as specified by the network parameter) belongs. If you do not specify an ID, the subscriber or the subscriber network becomes part of the default traffic domain.

aclname Name(s) of any configured extended ACL(s) whose action is ALLOW. The condition specified in the extended ACL rule identifies the traffic from an LSN subscriber for which the Citrix ADC is to perform large scale NAT.

acl6name Name of any configured extended ACL6 whose action is ALLOW. The condition specified in the extended ACL6 rule is used as the condition for the LSN client.

network6 IPv6 address(es) of the LSN subscriber(s) or subscriber network(s) on whose traffic you want the Citrix ADC to perform Large Scale NAT.

clientType This field stores the type of lsn client. Initially it will be UNSET. Once network/acl is bound, appropriate type will be decided. Primarily useful in DB validation case.

devno count stateflag

Example

show lsn client client1

unbind lsn client

Unbind LSN Client with client network or host.

Synopsis

unbind lsn client <clientname> ((-network <ip_addr>) | -aclname <string> | -network6 <ipv6_addr|*> | -acl6name <string>)

Arguments

clientname Name for the LSN client entity. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN client is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn client1" or 'lsn client1').

network IPv4 address(es) of the LSN subscriber(s) or subscriber network(s) on whose traffic you want the Citrix ADC to perform Large Scale NAT.

netmask Subnet mask for the IPv4 address specified in the Network parameter. Default value: 0xFFFFFFFF

aclname Name(s) of any configured extended ACL(s) whose action is ALLOW. The condition specified in the extended ACL rule identifies the traffic from an LSN subscriber for which the Citrix ADC is to perform large scale NAT.

acl6name Name of any configured extended ACL6 whose action is ALLOW. The condition specified in the extended ACL6 rule is used as the condition for the LSN client.

network6 IPv6 address(es) of the LSN subscriber(s) or subscriber network(s) on whose traffic you want the Citrix ADC to perform Large Scale NAT.

td ID of the traffic domain on which this subscriber or the subscriber network (as specified by the network parameter) belongs. If you do not specify an ID, the subscriber or the subscriber network becomes part of the default traffic domain. Default value: 0 Minimum value: 0 Maximum value: 4094

Example

unbind lsn client client1 -network 1.1.1.0 -netmask 255.255.255.0 -td 0

rm lsn client

Remove LSN Client.

Synopsis

rm lsn client <clientname>

Arguments

clientname Name for the LSN client entity. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN client is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn client1" or 'lsn client1').

Example

rm lsn client client1

bind lsn client

Bind LSN Client with client network or host. There can be a maximum of 1 million LSN subscribers globally.

Synopsis

bind lsn client <clientname> ((-network <ip_addr>) | -aclname <string> | -network6 <ipv6_addr|*> | -acl6name <string>)

Arguments

clientname Name for the LSN client entity. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN client is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn client1" or 'lsn client1').

network IPv4 address(es) of the LSN subscriber(s) or subscriber network(s) on whose traffic you want the Citrix ADC to perform Large Scale NAT.

netmask Subnet mask for the IPv4 address specified in the Network parameter. Default value: 0xFFFFFFFF

aclname Name(s) of any configured extended ACL(s) whose action is ALLOW. The condition specified in the extended ACL rule identifies the traffic from an LSN subscriber for which the Citrix ADC is to perform large scale NAT.

acl6name Name of any configured extended ACL6 whose action is ALLOW. The condition specified in the extended ACL6 rule is used as the condition for the LSN client.

network6 IPv6 address(es) of the LSN subscriber(s) or subscriber network(s) on whose traffic you want the Citrix ADC to perform Large Scale NAT.

td ID of the traffic domain on which this subscriber or the subscriber network (as specified by the network parameter) belongs. If you do not specify an ID, the subscriber or the subscriber network becomes part of the default traffic domain. Default value: 0 Minimum value: 0 Maximum value: 4094

Example

bind lsn client client1 -network 1.1.1.0 -netmask 255.255.255.0 -td 0

add lsn client

Add LSN Client.

Synopsis

add lsn client <clientname>

Arguments

clientname Name for the LSN client entity. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN client is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn client1" or 'lsn client1').

Example

add lsn client client1

Lsn

The entities on which you can perform NetScaler CLI operations:

- lsn-appsattributes
- lsn-appsprofile
- lsn-client
- lsn-deterministicNat
- lsn-dslite
- lsn-group
- lsn-httphdrlogprofile
- lsn-ip6profile
- lsn-logprofile
- lsn
- lsn-nat64
- lsn-parameter
- lsn-pool

- lsn-rtspalgprofile
- lsn-rtspalgsession
- lsn-session
- lsn-sipalgcall
- lsn-sipalgprofile
- lsn-static
- lsn-transportprofile

lsn-deterministicNat

The following operations can be performed on "lsn-deterministicNat":

show lsn deterministicNat

Show LSN deterministic.

Synopsis

show lsn deterministicNat (-clientname <string> | -network6 <ipv6_addr|*> | -natIP <ip_addr>) [-subscrIP <ip_addr>]

Arguments

clientname The name of the LSN Client.

network6 IPv6 address of the LSN subscriber or B4 device.

subscrIP The Client IP address.

td The LSN client TD. Default value: 0 Minimum value: 0 Maximum value: 4094

natIP The NAT IP address.

Output

natprefix IPv6 address of the LSN subscriber network(B4-Device) on whose traffic the Citrix ADC perform Large Scale NAT.

subscrIP The Subscriber IP address.

natIP The NAT IP address.

firstport The Application Protocol Port of the Profile.

lastport The Application Protocol Ending Port of the Profile.

srctd The LSN client TD.

nattype Type of subscriber info(ex: nat44 or ds-lite).

devno count stateflag

Example

show lsn deterministic

lsn-dslite

The following operations can be performed on "lsn-dslite":

stat lsn dslite

Display Large Scale NAT DS-Lite statistics.

Synopsis

stat lsn dslite

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

DS-Lite Received Packets (DSLiteRxPkts) Total number of LSN DS-Lite rx pkts.

DS-Lite Received Bytes (DSLiteRxBytes) Total number of LSN DS-Lite rx bytes.

DS-Lite Transmitted Packets (DSLiteTxPkts) Total number of LSN DS-Lite tx pkts.

DS-Lite Transmitted Bytes (DSLiteTxBytes) Total number of LSN DS-Lite tx bytes.

DS-Lite TCP Received Packets (DSLiteTcpRxPkts) Number of LSN DS-Lite TCP Received packets.

DS-Lite TCP Received Bytes (DSLiteTcpRxBytes) Number of LSN DS-Lite TCP Received bytes.

DS-Lite TCP Transmitted Packets (DSLiteTcpTxPkts) Number of LSN DS-Lite TCP Transmitted packets.

DS-Lite TCP Transmitted Bytes (DSLiteTcpTxBytes) Number of LSN DS-Lite TCP Transmitted bytes.

DS-Lite TCP Dropped Packets (DSLiteTcpDrpPkts) Number of LSN DS-Lite TCP Dropped packets.

DS-Lite TCP Current Sessions (DSLiteTcpSess) Number of LSN DS-Lite TCP Current Sessions.

DS-Lite UDP Received Packets (DSLiteUdpRxPkts) Number of LSN DS-Lite UDP Received packets.

DS-Lite UDP Received Bytes (DSLiteUdpRxBytes) Number of LSN DS-Lite UDP Received bytes.

DS-Lite UDP Transmitted Packets (DSLiteUdpTxPkts) Number of LSN DS-Lite UDP Transmitted packets.

DS-Lite UDP Transmitted Bytes (DSLiteUdpTxBytes) Number of LSN DS-Lite UDP Transmitted bytes.

DS-Lite UDP Dropped Packets (DSLiteUdpDrpPkts) Number of LSN DS-Lite UDP Dropped packets.

DS-Lite UDP Current Sessions (DSLiteUdpSess) Number of LSN DS-Lite UDP Current Sessions.

DS-Lite ICMP Received Packets (DSLiteIcmpRxPkts) Number of LSN DS-Lite ICMP Received packets.

DS-Lite ICMP Received Bytes (DSLiteIcmpRxBytes) Number of LSN DS-Lite ICMP Received bytes.

DS-Lite ICMP Transmitted Packets (DSLiteIcmpTxPkts) Number of LSN DS-Lite ICMP Transmitted packets.

DS-Lite ICMP Transmitted Bytes (DSLiteIcmpTxBytes) Number of LSN DS-Lite ICMP Transmitted bytes.

DS-Lite ICMP Dropped Packets (DSLiteIcmpDrpPkts) Number of LSN DS-Lite ICMP Dropped packets.

DS-Lite ICMP Current Sessions (DSLiteIcmpSess) Number of LSN DS-Lite ICMP Current Sessions.

DS-Lite Sessions (DSLiteSession) Current number of LSN DS-Lite sessions.

DS-Lite Subscribers (DSLiteSubscr) Current number of LSN DS-Lite subscribers.

Related Commands

- stat lsn nat64

lsn-group

The following operations can be performed on "lsn-group":

set| rm| show| unset| unbind| bind| add| stat|

set lsn group

Set LSN Group.

Synopsis

set lsn group <groupname>

Arguments

groupname Name for the LSN group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or

more spaces, enclose the name in double or single quotation marks (for example, "lsn group1" or 'lsn group1').

portblocksize Size of the NAT port block to be allocated for each subscriber.

To set this parameter for Dynamic NAT, you must enable the port block allocation parameter in the bound LSN pool. For Deterministic NAT, the port block allocation parameter is always enabled, and you cannot disable it.

In Dynamic NAT, the Citrix ADC allocates a random NAT port block, from the available NAT port pool of an NAT IP address, for each subscriber. For a subscriber, if all the ports are allocated from the subscriber's allocated port block, the ADC allocates a new random port block for the subscriber.

The default port block size is 256 for Deterministic NAT, and 0 for Dynamic NAT. Default value: 0 Minimum value: 256 Maximum value: 65536

logging Log mapping entries and sessions created or deleted for this LSN group. The Citrix ADC logs LSN sessions for this LSN group only when both logging and session logging parameters are enabled.

The ADC uses its existing syslog and audit log framework to log LSN information. You must enable global level LSN logging by enabling the LSN parameter in the related NSLOG action and SYLOG action entities. When the Logging parameter is enabled, the Citrix ADC generates log messages related to LSN mappings and LSN sessions of this LSN group. The ADC then sends these log messages to servers associated with the NSLOG action and SYSLOG actions entities.

A log message for an LSN mapping entry consists of the following information:

- NSIP address of the Citrix ADC
- Time stamp
- Entry type (MAPPING or SESSION)
- Whether the LSN mapping entry is created or deleted
- Subscriber's IP address, port, and traffic domain ID
- NAT IP address and port
- Protocol name
- Destination IP address, port, and traffic domain ID might be present, depending on the following conditions: `Destination IP address and port are not logged for Endpoint-Independent mapping` Only Destination IP address (and not port) is logged for Address-

Dependent mapping ` Destination IP address and port are logged for Address-Port-Dependent mapping

Possible values: ENABLED, DISABLED Default value: DISABLED

sessionLogging Log sessions created or deleted for the LSN group. The Citrix ADC logs LSN sessions for this LSN group only when both logging and session logging parameters are enabled.

A log message for an LSN session consists of the following information:

- NSIP address of the Citrix ADC
- Time stamp
- Entry type (MAPPING or SESSION)
- Whether the LSN session is created or removed
- Subscriber's IP address, port, and traffic domain ID
- NAT IP address and port
- Protocol name
- Destination IP address, port, and traffic domain ID

Possible values: ENABLED, DISABLED Default value: DISABLED

sessionSync In a high availability (HA) deployment, synchronize information of all LSN sessions related to this LSN group with the secondary node. After a failover, established TCP connections and UDP packet flows are kept active and resumed on the secondary node (new primary).

For this setting to work, you must enable the global session synchronization parameter.

Possible values: ENABLED, DISABLED Default value: ENABLED

snmptraplimit Maximum number of SNMP Trap messages that can be generated for the LSN group in one minute. Default value: 100 Minimum value: 0 Maximum value: 10000

ftp Enable Application Layer Gateway (ALG) for the FTP protocol. For some application-layer protocols, the IP addresses and protocol port numbers are usually communicated in the packet's payload. When acting as an ALG, the Citrix ADC changes the packet's payload to ensure that the protocol continues to work over LSN.

Note: The Citrix ADC also includes ALG for ICMP and TFTP protocols. ALG for the ICMP protocol is enabled by default, and there is no provision to disable it. ALG for the TFTP protocol is disabled by default. ALG is enabled automatically for an LSN group when you bind a UDP LSN application

profile, with endpoint-independent-mapping, endpoint-independent filtering, and destination port as 69 (well-known port for TFTP), to the LSN group.

Possible values: ENABLED, DISABLED Default value: ENABLED

pptp Enable the PPTP Application Layer Gateway.

Possible values: ENABLED, DISABLED Default value: DISABLED

sipalg Enable the SIP ALG.

Possible values: ENABLED, DISABLED Default value: DISABLED

rtspalg Enable the RTSP ALG.

Possible values: ENABLED, DISABLED Default value: DISABLED

ftpcm Enable the FTP connection mirroring for specified LSN group. Connection mirroring (CM or connection failover) refers to keeping active an established TCP or UDP connection when a failover occurs.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set lsn group group1

rm lsn group

Remove LSN Group.

Synopsis

rm lsn group <groupname>

Arguments

groupname Name for the LSN group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn group1" or 'lsn group1').

Example

rm lsn group group1

show lsn group

Display LSN Group.

Synopsis

show lsn group

Arguments

groupname Name for the LSN group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn group1" or 'lsn group1').

Output

poolname Name of the LSN pool to bind to the specified LSN group. Only LSN Pools and LSN groups with the same NAT type settings can be bound together. Multiples LSN pools can be bound to an LSN group.

For Deterministic NAT, pools bound to an LSN group cannot be bound to other LSN groups. For Dynamic NAT, pools bound to an LSN group can be bound to multiple LSN groups.

transportprofilename Name of the LSN transport profile to bind to the specified LSN group. Bind a profile for each protocol for which you want to specify settings.

By default, one LSN transport profile with default settings for TCP, UDP, and ICMP protocols is bound to an LSN group during its creation. This profile is called a default transport.

An LSN transport profile that you bind to an LSN group overrides the default LSN transport profile for that protocol.

appsprofilename Name of the LSN application profile to bind to the specified LSN group. For each set of destination ports, bind a profile for each protocol for which you want to specify settings.

By default, one LSN application profile with default settings for TCP, UDP, and ICMP protocols for all destination ports is bound to an LSN group during its creation. This profile is called a default application profile.

When you bind an LSN application profile, with a specified set of destination ports, to an LSN group, the bound profile overrides the default LSN application profile for that protocol at that set of destination ports.

clientname Name of the LSN client entity to be associated with the LSN group. You can associate only one LSN client entity with an LSN group.You cannot remove this association or replace with another LSN client entity once the LSN group is created.

nattype Type of NAT IP address and port allocation (from the bound LSN pools) for subscribers:

Available options function as follows:

- Deterministic - Allocate a NAT IP address and a block of ports to each subscriber (of the LSN client bound to the LSN group). The Citrix ADC sequentially allocates NAT resources to these subscribers. The Citrix ADC ADC assigns the first block of ports (block size determined by the port block size parameter of the LSN group) on the beginning NAT IP address to the beginning subscriber IP address. The next range of ports is assigned to the next subscriber, and so on, until the NAT address does not have enough ports for the next subscriber. In this case, the first port block on the next NAT address is used for the subscriber, and so on. Because each subscriber now receives a deterministic NAT IP address and a block of ports, a subscriber can be identified without any need for logging. For a connection, a subscriber can be identified based only on the NAT IP address and port, and the destination IP address and port. The maximum number of LSN subscribers allowed, globally, is 1 million.
- Dynamic - Allocate a random NAT IP address and a port from the LSN NAT pool for a subscriber's connection. If port block allocation is enabled (in LSN pool) and a port block size is specified (in the LSN group), the Citrix ADC allocates a random NAT IP address and a block of ports for a subscriber when it initiates a connection for the first time. The ADC allocates this NAT IP address and a port (from the allocated block of ports) for different connections from this subscriber. If all the ports are allocated (for different subscriber's connections) from the subscriber's allocated port block, the ADC allocates a new random port block for the subscriber.

allocPolicy NAT IP and PORT block allocation policy for Deterministic NAT. Supported Policies are, 1: PORTS: Port blocks from single NATIP will be allocated to LSN subscribers sequentially. After all blocks are exhausted, port blocks from next NATIP will be allocated and so on. 2: IPADDRS(Default): One port block from each NATIP will be allocated and once all the NATIPs are over second port block from each NATIP will be allocated and so on. To understand better if we

assume port blocks of all NAT IPs as two dimensional array, PORTS policy follows "row major order" and IPADDRS policy follows "column major order" while allocating port blocks. Example: Client IPs: 2.2.2.1, 2.2.2.2 and 2.2.2.3 NAT IPs and PORT Blocks: 4.4.4.1:PB1, PB2, PB3,., PBn 4.4.4.2: PB1, PB2, PB3,., PBn PORTS Policy: 2.2.2.1 => 4.4.4.1:PB1 2.2.2.2 => 4.4.4.1:PB2 2.2.2.3 => 4.4.4.1:PB3 IPADDRS Policy: 2.2.2.1 => 4.4.4.1:PB1 2.2.2.2 => 4.4.4.2:PB1 2.2.2.3 => 4.4.4.1:PB2

portblocksize Size of the NAT port block to be allocated for each subscriber.

To set this parameter for Dynamic NAT, you must enable the port block allocation parameter in the bound LSN pool. For Deterministic NAT, the port block allocation parameter is always enabled, and you cannot disable it.

In Dynamic NAT, the Citrix ADC allocates a random NAT port block, from the available NAT port pool of an NAT IP address, for each subscriber. For a subscriber, if all the ports are allocated from the subscriber's allocated port block, the ADC allocates a new random port block for the subscriber.

The default port block size is 256 for Deterministic NAT, and 0 for Dynamic NAT.

logging Log mapping entries and sessions created or deleted for this LSN group. The Citrix ADC logs LSN sessions for this LSN group only when both logging and session logging parameters are enabled.

The ADC uses its existing syslog and audit log framework to log LSN information. You must enable global level LSN logging by enabling the LSN parameter in the related NSLOG action and SYLOG action entities. When the Logging parameter is enabled, the Citrix ADC generates log messages related to LSN mappings and LSN sessions of this LSN group. The ADC then sends these log messages to servers associated with the NSLOG action and SYSLOG actions entities.

A log message for an LSN mapping entry consists of the following information:

- NSIP address of the Citrix ADC
- Time stamp
- Entry type (MAPPING or SESSION)
- Whether the LSN mapping entry is created or deleted
- Subscriber's IP address, port, and traffic domain ID
- NAT IP address and port
- Protocol name

- Destination IP address, port, and traffic domain ID might be present, depending on the following conditions: `Destination IP address and port are not logged for Endpoint-Independent mapping` Only Destination IP address (and not port) is logged for Address-Dependent mapping ` Destination IP address and port are logged for Address-Port-Dependent mapping

sessionLogging Log sessions created or deleted for the LSN group. The Citrix ADC logs LSN sessions for this LSN group only when both logging and session logging parameters are enabled.

A log message for an LSN session consists of the following information:

- NSIP address of the Citrix ADC
- Time stamp
- Entry type (MAPPING or SESSION)
- Whether the LSN session is created or removed
- Subscriber's IP address, port, and traffic domain ID
- NAT IP address and port
- Protocol name
- Destination IP address, port, and traffic domain ID

sessionSync In a high availability (HA) deployment, synchronize information of all LSN sessions related to this LSN group with the secondary node. After a failover, established TCP connections and UDP packet flows are kept active and resumed on the secondary node (new primary).

For this setting to work, you must enable the global session synchronization parameter.

snmptraplimit Maximum number of SNMP Trap messages that can be generated for the LSN group in one minute.

ftp Enable Application Layer Gateway (ALG) for the FTP protocol. For some application-layer protocols, the IP addresses and protocol port numbers are usually communicated in the packet's payload. When acting as an ALG, the Citrix ADC changes the packet's payload to ensure that the protocol continues to work over LSN.

Note: The Citrix ADC also includes ALG for ICMP and TFTP protocols. ALG for the ICMP protocol is enabled by default, and there is no provision to disable it. ALG for the TFTP protocol is disabled by default. ALG is enabled automatically for an LSN group when you bind a UDP LSN application

profile, with endpoint-independent-mapping, endpoint-independent filtering, and destination port as 69 (well-known port for TFTP), to the LSN group.

pptp Enable the PPTP Application Layer Gateway.

groupId sipalg Enable the SIP ALG.

sipalgprofilename The name of the LSN SIP ALG Profile.

rtspalg Enable the RTSP ALG.

rtspalgprofilename The name of the LSN RTSP ALG Profile.

ip6profile Name of the LSN ip6 profile to associate with the specified LSN group. An ip6 profile can be associated with a group only during group creation.

By default, no LSN ip6 profile is associated with an LSN group during its creation. Only one ip6profile can be associated with a group.

httphdrlogprofilename The name of the LSN HTTP header logging Profile.

pcpServer Name of the PCP server to be associated with lsn group.

logProfileName The name of the LSN logging Profile.

ipsecAlgProfile Name of the IPSec ALG profile to bind to the specified LSN group.

ftpcm Enable the FTP connection mirroring for specified LSN group. Connection mirroring (CM or connection failover) refers to keeping active an established TCP or UDP connection when a failover occurs.

devno count stateflag

Example

show lsn group group1

unset lsn group

Use this command to remove lsn group settings.Refer to the set lsn group command for meanings of the arguments.

Synopsis

unset lsn group <groupname>

unbind lsn group

Unbind LSN Group with protocol profiles and pools.

Synopsis

unbind lsn group <groupname> (-poolname <string> | -transportprofilename <string> | -ipsecAlgProfile <string> | -httphdrlogprofilename <string> | -appsprofilename <string> | -sipalgprofilename <string> | -rtspalgprofilename <string> | -pcpServer <string> | -logProfileName <string>)

Arguments

groupname Name for the LSN group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn group1" or 'lsn group1').

poolname Name of the LSN pool to bind to the specified LSN group. Only LSN Pools and LSN groups with the same NAT type settings can be bound together. Multiples LSN pools can be bound to an LSN group.

For Deterministic NAT, pools bound to an LSN group cannot be bound to other LSN groups. For Dynamic NAT, pools bound to an LSN group can be bound to multiple LSN groups.

transportprofilename Name of the LSN transport profile to bind to the specified LSN group. Bind a profile for each protocol for which you want to specify settings.

By default, one LSN transport profile with default settings for TCP, UDP, and ICMP protocols is bound to an LSN group during its creation. This profile is called a default transport.

An LSN transport profile that you bind to an LSN group overrides the default LSN transport profile for that protocol.

ipsecAlgProfile Name of the IPSec ALG profile to bind to the specified LSN group.

httphdrlogprofilename The name of the LSN HTTP header logging Profile.

appsprofilename Name of the LSN application profile to bind to the specified LSN group. For each set of destination ports, bind a profile for each protocol for which you want to specify settings.

By default, one LSN application profile with default settings for TCP, UDP, and ICMP protocols for all destination ports is bound to an LSN group during its creation. This profile is called a default application profile.

When you bind an LSN application profile, with a specified set of destination ports, to an LSN group, the bound profile overrides the default LSN application profile for that protocol at that set of destination ports.

sipalgprofilename The name of the LSN SIP ALG Profile.

rtspalgprofilename The name of the LSN RTSP ALG Profile.

pcpServer Name of the PCP server to be associated with lsn group.

logProfileName The name of the LSN logging Profile.

Example

unbind lsn group group1 -transportprofile profile1 -appsprofile profile2

bind lsn group

Bind LSN Group with protocol profiles and pools.

Synopsis

bind lsn group <groupname> (-poolname <string> | -transportprofilename <string> | -ipsecAlgProfile <string> | -httphdrlogprofilename <string> | -appsprofilename <string> | -sipalgprofilename <string> | -rtspalgprofilename <string> | -pcpServer <string> | -logProfileName <string>)

Arguments

groupname Name for the LSN group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn group1" or 'lsn group1').

poolname Name of the LSN pool to bind to the specified LSN group. Only LSN Pools and LSN groups with the same NAT type settings can be bound together. Multiples LSN pools can be bound to an LSN group.

For Deterministic NAT, pools bound to an LSN group cannot be bound to other LSN groups. For Dynamic NAT, pools bound to an LSN group can be bound to multiple LSN groups.

transportprofilename Name of the LSN transport profile to bind to the specified LSN group. Bind a profile for each protocol for which you want to specify settings.

By default, one LSN transport profile with default settings for TCP, UDP, and ICMP protocols is bound to an LSN group during its creation. This profile is called a default transport.

An LSN transport profile that you bind to an LSN group overrides the default LSN transport profile for that protocol.

ipsecAlgProfile Name of the IPSec ALG profile to bind to the specified LSN group.

httphdrlogprofilename The name of the LSN HTTP header logging Profile.

appsprofilename Name of the LSN application profile to bind to the specified LSN group. For each set of destination ports, bind a profile for each protocol for which you want to specify settings.

By default, one LSN application profile with default settings for TCP, UDP, and ICMP protocols for all destination ports is bound to an LSN group during its creation. This profile is called a default application profile.

When you bind an LSN application profile, with a specified set of destination ports, to an LSN group, the bound profile overrides the default LSN application profile for that protocol at that set of destination ports.

sipalgprofilename The name of the LSN SIP ALG Profile.

rtspalgprofilename The name of the LSN RTSP ALG Profile.

pcpServer Name of the PCP server to be associated with lsn group.

logProfileName The name of the LSN logging Profile.

Example

bind lsn group group1 -transportprofile profile1 -appsprofile profile2

add lsn group

Add LSN Group.

Synopsis

add lsn group <groupname> -clientname <string> [-nattype (DYNAMIC | DETERMINISTIC)]

Arguments

groupname Name for the LSN group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn group1" or 'lsn group1').

clientname Name of the LSN client entity to be associated with the LSN group. You can associate only one LSN client entity with an LSN group.You cannot remove this association or replace with another LSN client entity once the LSN group is created.

nattype Type of NAT IP address and port allocation (from the bound LSN pools) for subscribers:

Available options function as follows:

- Deterministic - Allocate a NAT IP address and a block of ports to each subscriber (of the LSN client bound to the LSN group). The Citrix ADC sequentially allocates NAT resources to these subscribers. The Citrix ADC ADC assigns the first block of ports (block size determined by the port block size parameter of the LSN group) on the beginning NAT IP address to the beginning subscriber IP address. The next range of ports is assigned to the next subscriber, and so on, until the NAT address does not have enough ports for the next subscriber. In this case, the first port block on the next NAT address is used for the subscriber, and so on. Because each subscriber now receives a deterministic NAT IP address and a block of ports, a subscriber can be identified without any need for logging. For a connection, a subscriber can be identified based only on the NAT IP address and port, and the destination IP address and port. The maximum number of LSN subscribers allowed, globally, is 1 million.
- Dynamic - Allocate a random NAT IP address and a port from the LSN NAT pool for a subscriber's connection. If port block allocation is enabled (in LSN pool) and a port block size is specified (in the LSN group), the Citrix ADC allocates a random NAT IP address and a block of ports for a subscriber when it initiates a connection for the first time. The ADC allocates this NAT IP address and a port (from the allocated block of ports) for different connections from this subscriber. If all the ports are allocated (for different subscriber's connections) from the subscriber's allocated port block, the ADC allocates a new random port block for the subscriber.

Possible values: DYNAMIC, DETERMINISTIC Default value: DYNAMIC

allocPolicy NAT IP and PORT block allocation policy for Deterministic NAT. Supported Policies are, 1: PORTS: Port blocks from single NATIP will be allocated to LSN subscribers sequentially. After all blocks are exhausted, port blocks from next NATIP will be allocated and so on. 2: IPADDRS(Default): One port block from each NATIP will be allocated and once all the NATIPs are over second port block from each NATIP will be allocated and so on. To understand better if we assume port blocks of all NAT IPs as two dimensional array, PORTS policy follows "row major order" and IPADDRS policy follows "column major order" while allocating port blocks. Example: Client IPs: 2.2.2.1, 2.2.2.2 and 2.2.2.3 NAT IPs and PORT Blocks: 4.4.4.1:PB1, PB2, PB3,., PBn 4.4.4.2: PB1, PB2, PB3,., PBn PORTS Policy: 2.2.2.1 => 4.4.4.1:PB1 2.2.2.2 => 4.4.4.1:PB2 2.2.2.3 => 4.4.4.1:PB3 IPADDRS Policy: 2.2.2.1 => 4.4.4.1:PB1 2.2.2.2 => 4.4.4.2:PB1 2.2.2.3 => 4.4.4.1:PB2

Possible values: PORTS, IPADDRS Default value: PORTS

portblocksize Size of the NAT port block to be allocated for each subscriber.

To set this parameter for Dynamic NAT, you must enable the port block allocation parameter in the bound LSN pool. For Deterministic NAT, the port block allocation parameter is always enabled, and you cannot disable it.

In Dynamic NAT, the Citrix ADC allocates a random NAT port block, from the available NAT port pool of an NAT IP address, for each subscriber. For a subscriber, if all the ports are allocated from the subscriber's allocated port block, the ADC allocates a new random port block for the subscriber.

The default port block size is 256 for Deterministic NAT, and 0 for Dynamic NAT. Default value: 0 Minimum value: 256 Maximum value: 65536

logging Log mapping entries and sessions created or deleted for this LSN group. The Citrix ADC logs LSN sessions for this LSN group only when both logging and session logging parameters are enabled.

The ADC uses its existing syslog and audit log framework to log LSN information. You must enable global level LSN logging by enabling the LSN parameter in the related NSLOG action and SYLOG action entities. When the Logging parameter is enabled, the Citrix ADC generates log messages related to LSN mappings and LSN sessions of this LSN group. The ADC then sends these log messages to servers associated with the NSLOG action and SYSLOG actions entities.

A log message for an LSN mapping entry consists of the following information:

- NSIP address of the Citrix ADC
- Time stamp

- Entry type (MAPPING or SESSION)
- Whether the LSN mapping entry is created or deleted
- Subscriber's IP address, port, and traffic domain ID
- NAT IP address and port
- Protocol name
- Destination IP address, port, and traffic domain ID might be present, depending on the following conditions: `Destination IP address and port are not logged for Endpoint-Independent mapping` Only Destination IP address (and not port) is logged for Address-Dependent mapping ` Destination IP address and port are logged for Address-Port-Dependent mapping

Possible values: ENABLED, DISABLED Default value: DISABLED

sessionLogging Log sessions created or deleted for the LSN group. The Citrix ADC logs LSN sessions for this LSN group only when both logging and session logging parameters are enabled.

A log message for an LSN session consists of the following information:

- NSIP address of the Citrix ADC
- Time stamp
- Entry type (MAPPING or SESSION)
- Whether the LSN session is created or removed
- Subscriber's IP address, port, and traffic domain ID
- NAT IP address and port
- Protocol name
- Destination IP address, port, and traffic domain ID

Possible values: ENABLED, DISABLED Default value: DISABLED

sessionSync In a high availability (HA) deployment, synchronize information of all LSN sessions related to this LSN group with the secondary node. After a failover, established TCP connections and UDP packet flows are kept active and resumed on the secondary node (new primary).

For this setting to work, you must enable the global session synchronization parameter.

Possible values: ENABLED, DISABLED Default value: ENABLED

snmptraplimit Maximum number of SNMP Trap messages that can be generated for the LSN group in one minute. Default value: 100 Minimum value: 0 Maximum value: 10000

ftp Enable Application Layer Gateway (ALG) for the FTP protocol. For some application-layer protocols, the IP addresses and protocol port numbers are usually communicated in the packet's payload. When acting as an ALG, the Citrix ADC changes the packet's payload to ensure that the protocol continues to work over LSN.

Note: The Citrix ADC also includes ALG for ICMP and TFTP protocols. ALG for the ICMP protocol is enabled by default, and there is no provision to disable it. ALG for the TFTP protocol is disabled by default. ALG is enabled automatically for an LSN group when you bind a UDP LSN application profile, with endpoint-independent-mapping, endpoint-independent filtering, and destination port as 69 (well-known port for TFTP), to the LSN group.

Possible values: ENABLED, DISABLED Default value: ENABLED

pptp Enable the PPTP Application Layer Gateway.

Possible values: ENABLED, DISABLED Default value: DISABLED

sipalg Enable the SIP ALG.

Possible values: ENABLED, DISABLED Default value: DISABLED

rtspalg Enable the RTSP ALG.

Possible values: ENABLED, DISABLED Default value: DISABLED

ip6profile Name of the LSN ip6 profile to associate with the specified LSN group. An ip6 profile can be associated with a group only during group creation.

By default, no LSN ip6 profile is associated with an LSN group during its creation. Only one ip6profile can be associated with a group.

ftpcm Enable the FTP connection mirroring for specified LSN group. Connection mirroring (CM or connection failover) refers to keeping active an established TCP or UDP connection when a failover occurs.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

add lsn group group1

stat lsn group

Display statistics for all LSN groups or display detailed statistics for the specified LSN group.

Synopsis

stat lsn group

Arguments

groupname Name of the LSN Group.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Current Sessions (Session) Number of Current Sessions for LSN group

Translated Bytes (Bytes) Number of Translated Bytes for LSN group

Translated Pkts (Pkts) Number of Translated Pkts for LSN group

TCP Translated Pkts (TcpTranslPkts) Number of TCP Translated Pkts for LSN group

TCP Translated Bytes (TcpTranslBytes) Number of TCP Translated Bytes for LSN group

TCP Dropped Pkts (TcpDrpPkts) Number of TCP Dropped Pkts for LSN group

TCP Current Sessions (TcpSess) Number of TCP Current Sessions for LSN group

UDP Translated Pkts (UdpTranslPkts) Number of UDP Translated Pkts for LSN group

UDP Translated Bytes (UdpTranslBytes) Number of UDP Translated Bytes for LSN group

UDP Dropped Pkts (UdpDrpPkts) Number of UDP Dropped Pkts for LSN group

UDP Current Sessions (UdpSess) Number of UDP Current Sessions for LSN group

ICMP Translated Pkts (IcmpTranslPkts) Number of ICMP Translated Pkts for LSN group

ICMP Translated Bytes (IcmpTranslBytes) Number of ICMP Translated Bytes for LSN group

ICMP Dropped Pkts (IcmpDrpPkts) Number of ICMP Dropped Pkts for LSN group

ICMP Current Sessions (IcmpSess) Number of ICMP Current Sessions for LSN group

Current Subscribers (Subscr) Number of ICMP Current Sessions for LSN group

Related Commands

- stat lsn nat64

lsn-httphdrlogprofile

The following operations can be performed on "lsn-httphdrlogprofile":

set| add| unset| rm| show|

set lsn httphdrlogprofile

Set LSN HTTP header logging Profile.

Synopsis

set lsn httphdrlogprofile <httphdrlogprofilename>

Arguments

httphdrlogprofilename The name of the HTTP header logging Profile.

logURL URL information is logged if option is enabled.

Possible values: ENABLED, DISABLED Default value: ENABLED

logMethod HTTP method information is logged if option is enabled.

Possible values: ENABLED, DISABLED Default value: ENABLED

logVersion Version information is logged if option is enabled.

Possible values: ENABLED, DISABLED Default value: ENABLED

logHost Host information is logged if option is enabled.

Possible values: ENABLED, DISABLED Default value: ENABLED

Example

set lsn transportprofile profile1 -portquota 128

add lsn httphdrlogprofile

Add LSN HTTP header logging Profile.

Synopsis

add lsn httphdrlogprofile <httphdrlogprofilename>

Arguments

httphdrlogprofilename The name of the HTTP header logging Profile.

logURL URL information is logged if option is enabled.

Possible values: ENABLED, DISABLED Default value: ENABLED

logMethod HTTP method information is logged if option is enabled.

Possible values: ENABLED, DISABLED Default value: ENABLED

logVersion Version information is logged if option is enabled.

Possible values: ENABLED, DISABLED Default value: ENABLED

logHost Host information is logged if option is enabled.

Possible values: ENABLED, DISABLED Default value: ENABLED

Example

add lsn httphdrlogprofile profile1 -url ENABLED

unset lsn httphdrlogprofile

Use this command to remove lsn httphdrlogprofile settings.Refer to the set lsn httphdrlogprofile command for meanings of the arguments.

Synopsis

unset lsn httphdrlogprofile <httphdrlogprofilename>

rm lsn httphdrlogprofile

Remove LSN HTTP header logging Profile.

Synopsis

rm lsn httphdrlogprofile <httphdrlogprofilename>

Arguments

httphdrlogprofilename The name of the HTTP header logging Profile.

Example

rm lsn transportprofile profile1

show lsn httphdrlogprofile

Display LSN HTTP header logging Profile.

Synopsis

show lsn httphdrlogprofile

Arguments

httphdrlogprofilename The name of the HTTP header logging Profile.

Output

logURL URL information is logged if option is enabled.

logMethod HTTP method information is logged if option is enabled.

logVersion Version information is logged if option is enabled.

logHost Host information is logged if option is enabled.

devno count stateflag

Example

show lsn transportprofile profile1

lsn-ip6profile

The following operations can be performed on "lsn-ip6profile":

rm| add| show|

rm lsn ip6profile

Remove LSN IP6Profile.

Synopsis

rm lsn ip6profile <name>

Arguments

name Name for the LSN ip6 profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN ip6 profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn ip6 profile1" or 'lsn ip6 profile1').

Example

rm lsn ip6profile i1

add lsn ip6profile

Add LSN IP6 profile.

Synopsis

add lsn ip6profile <name> -type (DS-Lite | NAT64)

Arguments

name Name for the LSN ip6 profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN ip6 profile is created. The following requirement applies only to the Citrix ADC CLI: If the name

includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn ip6 profile1" or 'lsn ip6 profile1').

type IPv6 translation type for which to set the LSN IP6 profile parameters.

Possible values: DS-Lite, NAT64

natprefix IPv6 address(es) of the LSN subscriber(s) or subscriber network(s) on whose traffic you want the Citrix ADC to perform Large Scale NAT.

network6 IPv6 address of the Citrix ADC AFTR device

Example

add lsn ip6profile i1 -type DS-Lite -network6 1001::1/64

show lsn ip6profile

Display LSN IP6 profile.

Synopsis

show lsn ip6profile

Arguments

name Name for the LSN ip6 profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN ip6 profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn ip6 profile1" or 'lsn ip6 profile1').

Output

type IPv6 translation type for which to set the LSN IP6 profile parameters.

network6 IPv6 address of the Citrix ADC AFTR device

natprefix IPv6 address(es) of the LSN subscriber(s) or subscriber network(s) on whose traffic you want the Citrix ADC to perform Large Scale NAT.

devno count stateflag

Example

show lsn ip6 profile

lsn-logprofile

The following operations can be performed on "lsn-logprofile":

unset| show| set| rm| add|

unset lsn logprofile

Use this command to remove lsn logprofile settings.Refer to the set lsn logprofile command for meanings of the arguments.

Synopsis

unset lsn logprofile <logProfileName>

show lsn logprofile

Display LSN logging Profile.

Synopsis

show lsn logprofile

Arguments

logProfileName The name of the logging Profile.

Output

logSubscrInfo Subscriber ID information is logged if option is enabled.

logCompact Logs in Compact Logging format if option is enabled.

logipfix Logs in IPFIX format if option is enabled.

analyticsProfile Name of the Analytics Profile attached to this lsn profile.

logSessDeletion LSN Session deletion will not be logged if disabled.

devno count stateflag

Example

show lsn logprofile profile1

set lsn logprofile

Set LSN logging Profile.

Synopsis

set lsn logprofile <logProfileName>

Arguments

logProfileName The name of the logging Profile.

logSubscrInfo Subscriber ID information is logged if option is enabled.

Possible values: ENABLED, DISABLED Default value: DISABLED

logCompact Logs in Compact Logging format if option is enabled.

Possible values: ENABLED, DISABLED Default value: ENABLED

logipfix Logs in IPFIX format if option is enabled.

Possible values: ENABLED, DISABLED Default value: DISABLED

analyticsProfile Name of the Analytics Profile attached to this lsn profile.

logSessDeletion LSN Session deletion will not be logged if disabled.

Possible values: ENABLED, DISABLED Default value: ENABLED

Example

set lsn logprofile profile1 -logSubscrInfo ENABLED

rm lsn logprofile

Remove LSN logging Profile.

Synopsis

rm lsn logprofile <logProfileName>

Arguments

logProfileName The name of the logging Profile.

Example

rm lsn logprofile profile1

add lsn logprofile

Add LSN logging Profile.

Synopsis

add lsn logprofile <logProfileName> [-logipfix (ENABLED | DISABLED)]

Arguments

logProfileName The name of the logging Profile.

logSubscrInfo Subscriber ID information is logged if option is enabled.

Possible values: ENABLED, DISABLED Default value: DISABLED

logCompact Logs in Compact Logging format if option is enabled.

Possible values: ENABLED, DISABLED Default value: ENABLED

logipfix Logs in IPFIX format if option is enabled.

Possible values: ENABLED, DISABLED Default value: DISABLED

analyticsProfile Name of the Analytics Profile attached to this lsn profile.

logSessDeletion LSN Session deletion will not be logged if disabled.

Possible values: ENABLED, DISABLED Default value: ENABLED

Example

add lsn logprofile profile1 -logSubscrInfo ENABLED

lsn-nat64

The following operations can be performed on "lsn-nat64":

stat lsn nat64

Display Large Scale NAT64 statistics.

Synopsis

stat lsn nat64

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

NAT64 Sessions (NAT64Session) Current number of LSN NAT64 sessions.

NAT64 Subscribers (NAT64Subscr) Current number of LSN NAT64 subscribers.

NAT64 Received Packets (NAT64RxPkts) Total number of LSN NAT64 rx pkts.

NAT64 Received Bytes (NAT64RxBytes) Total number of LSN NAT64 rx bytes.

NAT64 Transmitted Packets (NAT64TxPkts) Total number of LSN NAT64 tx pkts.

NAT64 Transmitted Bytes (NAT64TxBytes) Total number of LSN NAT64 tx bytes.

NAT64 TCP Current Sessions (NAT64TCPSess) Number of LSN NAT64 TCP Current Sessions.

NAT64 TCP Received Packets (NAT64TcpRxPkts) Number of LSN NAT64 TCP Received packets.

NAT64 TCP Received Bytes (NAT64TCPRxBytes) Number of LSN NAT64 TCP Received bytes.

NAT64 TCP Transmitted Packets (NAT64TcpTxPkts) Number of LSN NAT64 TCP Transmitted packets.

NAT64 TCP Transmitted Bytes (NAT64TCPTxBytes) Number of LSN NAT64 TCP Transmitted bytes.

NAT64 TCP Dropped Packets (NAT64TCPDrpPkts) Number of LSN NAT64 TCP Dropped packets.

NAT64 UDP Current Sessions (NAT64UDPSess) Number of LSN NAT64 UDP Current Sessions.

NAT64 UDP Received Packets (NAT64UDPRxPkts) Number of LSN NAT64 UDP Received packets.

NAT64 UDP Received Bytes (NAT64UDPRxBytes) Number of LSN NAT64 UDP Received bytes.

NAT64 UDP Transmitted Packets (NAT64UDPTxPkts) Number of LSN NAT64 UDP Transmitted packets.

NAT64 UDP Transmitted Bytes (NAT64UDPTxBytes) Number of LSN NAT64 UDP Transmitted bytes.

NAT64 UDP Dropped Packets (NAT64UDPDrpPkts) Number of LSN NAT64 UDP Dropped packets.

NAT64 ICMP Current Sessions (NAT64ICMPSess) Number of LSN NAT64 ICMP Current Sessions.

NAT64 ICMP Received Packets (NAT64ICMPRxPkts) Number of LSN NAT64 ICMP Received packets.

NAT64 ICMP Received Bytes (NAT64ICMPRxBytes) Number of LSN NAT64 ICMP Received bytes.

NAT64 ICMP Transmitted Packets (NAT64ICMPTxPkts) Number of LSN NAT64 ICMP Transmitted packets.

NAT64 ICMP Transmitted Bytes (NAT64ICMPTxBytes) Number of LSN NAT64 ICMP Transmitted bytes.

NAT64 ICMP Dropped Packets (NAT64ICMPDrpPkts) Number of LSN NAT64 ICMP Dropped packets.

Related Commands

- stat lsn dslite

lsn-parameter

The following operations can be performed on "lsn-parameter":

show| unset| set|

show lsn parameter

Display the global configuration of the LSN.

Synopsis

show lsn parameter

Arguments

Output

memLimitActive Amount of actual memory reserved for the LSN feature.

The amount of active memory for the LSN feature might be less than the configured memory, because the available memory is shared across features.

maxMemLimit Maximum amount of Citrix ADC memory that can be reserved for the LSN feature.

memLimit Amount of Citrix ADC memory to reserve for the LSN feature, in multiples of 2MB.

Note: If you later reduce the value of this parameter, the amount of active memory is not reduced. Changing the configured memory limit can only increase the amount of active memory. This command is deprecated, use 'set extendedmemoryparam -memlimit' instead.

sessionSync Synchronize all LSN sessions with the secondary node in a high availability (HA) deployment (global synchronization). After a failover, established TCP connections and UDP packet flows are kept active and resumed on the secondary node (new primary).

The global session synchronization parameter and session synchronization parameters (group level) of all LSN groups are enabled by default.

For a group, when both the global level and the group level LSN session synchronization parameters are enabled, the primary node synchronizes information of all LSN sessions related to this LSN group with the secondary node.

subscrSessionRemoval LSN global setting for controlling subscriber aware session removal, when this is enabled, when ever the subscriber info is deleted from subscriber database, sessions corresponding to that subscriber will be removed. if this setting is disabled, subscriber sessions will be timed out as per the idle time out settings.

unset lsn parameter

Use this command to remove lsn parameter settings.Refer to the set lsn parameter command for meanings of the arguments.

Synopsis

unset lsn parameter

set lsn parameter

Modify the global configuration of the LSN.

Synopsis

set lsn parameter

Arguments

sessionSync Synchronize all LSN sessions with the secondary node in a high availability (HA) deployment (global synchronization). After a failover, established TCP connections and UDP packet flows are kept active and resumed on the secondary node (new primary).

The global session synchronization parameter and session synchronization parameters (group level) of all LSN groups are enabled by default.

For a group, when both the global level and the group level LSN session synchronization parameters are enabled, the primary node synchronizes information of all LSN sessions related to this LSN group with the secondary node.

Possible values: ENABLED, DISABLED Default value: ENABLED

subscrSessionRemoval LSN global setting for controlling subscriber aware session removal, when this is enabled, when ever the subscriber info is deleted from subscriber database, sessions

corresponding to that subscriber will be removed. if this setting is disabled, subscriber sessions will be timed out as per the idle time out settings.

Possible values: ENABLED, DISABLED Default value: DISABLED

lsn-pool

The following operations can be performed on "lsn-pool":

show| bind| unset| stat| unbind| set| add| rm|

show lsn pool

Display LSN Pool.

Synopsis

show lsn pool

Arguments

poolname Name for the LSN pool. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN pool is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn pool1" or 'lsn pool1').

Output

lsnip IPv4 address or a range of IPv4 addresses to be used as NAT IP address(es) for LSN. After the pool is created, these IPv4 addresses are added to the Citrix ADC as Citrix ADC owned IP address of type LSN. A maximum of 4096 IP addresses can be bound to an LSN pool. An LSN IP address associated with an LSN pool cannot be shared with other LSN pools. IP addresses specified for this parameter must not already exist on the Citrix ADC as any Citrix ADC owned IP addresses. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189. You can later remove some or all the LSN IP addresses from the pool, and add IP addresses to the LSN pool. By default , arp is enabled on LSN IP address but, you can disable it using command - "set ns ip"

nattype Type of NAT IP address and port allocation (from the LSN pools bound to an LSN group) for subscribers (of the LSN client entity bound to the LSN group):

Available options function as follows:

- Deterministic - Allocate a NAT IP address and a block of ports to each subscriber (of the LSN client bound to the LSN group). The Citrix ADC sequentially allocates NAT resources to these subscribers. The Citrix ADC ADC assigns the first block of ports (block size determined by the port block size parameter of the LSN group) on the beginning NAT IP address to the beginning subscriber IP address. The next range of ports is assigned to the next subscriber, and so on, until the NAT address does not have enough ports for the next subscriber. In this case, the first port block on the next NAT address is used for the subscriber, and so on. Because each subscriber now receives a deterministic NAT IP address and a block of ports, a subscriber can be identified without any need for logging. For a connection, a subscriber can be identified based only on the NAT IP address and port, and the destination IP address and port.
- Dynamic - Allocate a random NAT IP address and a port from the LSN NAT pool for a subscriber's connection. If port block allocation is enabled (in LSN pool) and a port block size is specified (in the LSN group), the Citrix ADC allocates a random NAT IP address and a block of ports for a subscriber when it initiates a connection for the first time. The ADC allocates this NAT IP address and a port (from the allocated block of ports) for different connections from this subscriber. If all the ports are allocated (for different subscriber's connections) from the subscriber's allocated port block, the ADC allocates a new random port block for the subscriber. Only LSN Pools and LSN groups with the same NAT type settings can be bound together. Multiples LSN pools can be bound to an LSN group. A maximum of 16 LSN pools can be bound to an LSN group.

portrealloctimeout The waiting time, in seconds, between deallocating LSN NAT ports (when an LSN mapping is removed) and reallocating them for a new LSN session. This parameter is necessary in order to prevent collisions between old and new mappings and sessions. It ensures that all established sessions are broken instead of redirected to a different subscriber. This is not applicable for ports used in:

- Deterministic NAT
- Address-Dependent filtering and Address-Port-Dependent filtering
- Dynamic NAT with port block allocation In these cases, ports are immediately reallocated.

maxPortReallocTmq Maximum number of ports for which the port reallocation timeout applies for each NAT IP address. In other words, the maximum deallocated-port queue size for which the reallocation timeout applies for each NAT IP address.

When the queue size is full, the next port deallocated is reallocated immediately for a new LSN session.

portblockallocation Allocate a random NAT port block, from the available NAT port pool of an NAT IP address, for each subscriber when the NAT allocation is set as Dynamic NAT. For any connection initiated from a subscriber, the Citrix ADC allocates a NAT port from the subscriber's allocated NAT port block to create the LSN session.

You must set the port block size in the bound LSN group. For a subscriber, if all the ports are allocated from the subscriber's allocated port block, the Citrix ADC allocates a new random port block for the subscriber.

For Deterministic NAT, this parameter is enabled by default, and you cannot disable it.

ownerNode ID(s) of cluster node(s) on which command is to be executed

firstip IPv4 address or a range of IPv4 addresses to be used as NAT IP address(es) for LSN. After the pool is created, these IPv4 addresses are added to the Citrix ADC as Citrix ADC owned IP address of type LSN. A maximum of 4096 IP addresses can be bound to an LSN pool. An LSN IP address associated with an LSN pool cannot be shared with other LSN pools. IP addresses specified for this parameter must not already exist on the Citrix ADC as any Citrix ADC owned IP addresses. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189. You can later remove some or all the LSN IP addresses from the pool, and add IP addresses to the LSN pool.

lastip IPv4 address or a range of IPv4 addresses to be used as NAT IP address(es) for LSN. After the pool is created, these IPv4 addresses are added to the Citrix ADC as Citrix ADC owned IP address of type LSN. A maximum of 4096 IP addresses can be bound to an LSN pool. An LSN IP address associated with an LSN pool cannot be shared with other LSN pools. IP addresses specified for this parameter must not already exist on the Citrix ADC as any Citrix ADC owned IP addresses. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189. You can later remove some or all the LSN IP addresses from the pool, and add IP addresses to the LSN pool.

totalpoolipsbound total number of nat ip addresses bound to lsn pool

devno count stateflag

Example

show lsn pool pool1

bind lsn pool

Bind LSN Pool with ip address range.

Synopsis

bind lsn pool <poolname>

Arguments

poolname Name for the LSN pool. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN pool is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn pool1" or 'lsn pool1').

ownerNode ID(s) of cluster node(s) on which command is to be executed Default value: -1 Minimum value: 0 Maximum value: 31

lsnip IPv4 address or a range of IPv4 addresses to be used as NAT IP address(es) for LSN. After the pool is created, these IPv4 addresses are added to the Citrix ADC as Citrix ADC owned IP address of type LSN. A maximum of 4096 IP addresses can be bound to an LSN pool. An LSN IP address associated with an LSN pool cannot be shared with other LSN pools. IP addresses specified for this parameter must not already exist on the Citrix ADC as any Citrix ADC owned IP addresses. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189. You can later remove some or all the LSN IP addresses from the pool, and add IP addresses to the LSN pool. By default , arp is enabled on LSN IP address but, you can disable it using command - "set ns ip"

Example

bind lsn pool pool1 1.1.1.1-1.1.1.20

unset lsn pool

Use this command to remove lsn pool settings.Refer to the set lsn pool command for meanings of the arguments.

Synopsis

unset lsn pool <poolname>

stat lsn pool

Display detailed statistics for the specified LSN pool.

Synopsis

stat lsn pool

Arguments

poolname Name of the LSN Pool.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Ports usage Non-TCP (%) (NonTcp %) Other protocols ports usage percentage in this pool.

Ports usage TCP (%) (Tcp %) TCP ports usage percentage in this pool.

Current port allocation (TCP) (CurPortAllocTcp) Current port allocation for tcp in this pool.

Current port allocation(Non-TCP) (CurPortAllocNonTCP) Current port allocation for other protocols in this pool.

Total IPs (TotIps) Total IPs in this pool.

Related Commands

- stat lsn nat64

unbind lsn pool

Unbind LSN Pool with ip address range.

Synopsis

unbind lsn pool <poolname>

Arguments

poolname Name for the LSN pool. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN pool is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn pool1" or 'lsn pool1').

ownerNode ID(s) of cluster node(s) on which command is to be executed Default value: -1 Minimum value: 0 Maximum value: 31

lsnip IPv4 address or a range of IPv4 addresses to be used as NAT IP address(es) for LSN. After the pool is created, these IPv4 addresses are added to the Citrix ADC as Citrix ADC owned IP address of type LSN. A maximum of 4096 IP addresses can be bound to an LSN pool. An LSN IP address associated with an LSN pool cannot be shared with other LSN pools. IP addresses specified for this parameter must not already exist on the Citrix ADC as any Citrix ADC owned IP addresses. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189. You can later remove some or all the LSN IP addresses from the pool, and add IP addresses to the LSN pool. By default , arp is enabled on LSN IP address but, you can disable it using command - "set ns ip"

Example

unbind lsn pool pool1 1.1.1.1-1.1.1.20

set lsn pool

Set LSN Pool.

Synopsis

set lsn pool <poolname>

Arguments

poolname Name for the LSN pool. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN pool is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or

more spaces, enclose the name in double or single quotation marks (for example, "lsn pool1" or 'lsn pool1').

portrealloctimeout The waiting time, in seconds, between deallocating LSN NAT ports (when an LSN mapping is removed) and reallocating them for a new LSN session. This parameter is necessary in order to prevent collisions between old and new mappings and sessions. It ensures that all established sessions are broken instead of redirected to a different subscriber. This is not applicable for ports used in:

- Deterministic NAT
- Address-Dependent filtering and Address-Port-Dependent filtering
- Dynamic NAT with port block allocation In these cases, ports are immediately reallocated. Default value: 0 Maximum value: 600

maxPortReallocTmq Maximum number of ports for which the port reallocation timeout applies for each NAT IP address. In other words, the maximum deallocated-port queue size for which the reallocation timeout applies for each NAT IP address.

When the queue size is full, the next port deallocated is reallocated immediately for a new LSN session. Default value: 65536 Minimum value: 0 Maximum value: 65536

Example

set lsn pool pool1 -portrealloctimeout 10

add lsn pool

Add LSN Pool.

Synopsis

add lsn pool <poolname>

Arguments

poolname Name for the LSN pool. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN pool is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn pool1" or 'lsn pool1').

nattype Type of NAT IP address and port allocation (from the LSN pools bound to an LSN group) for subscribers (of the LSN client entity bound to the LSN group):

Available options function as follows:

- Deterministic - Allocate a NAT IP address and a block of ports to each subscriber (of the LSN client bound to the LSN group). The Citrix ADC sequentially allocates NAT resources to these subscribers. The Citrix ADC ADC assigns the first block of ports (block size determined by the port block size parameter of the LSN group) on the beginning NAT IP address to the beginning subscriber IP address. The next range of ports is assigned to the next subscriber, and so on, until the NAT address does not have enough ports for the next subscriber. In this case, the first port block on the next NAT address is used for the subscriber, and so on. Because each subscriber now receives a deterministic NAT IP address and a block of ports, a subscriber can be identified without any need for logging. For a connection, a subscriber can be identified based only on the NAT IP address and port, and the destination IP address and port.
- Dynamic - Allocate a random NAT IP address and a port from the LSN NAT pool for a subscriber's connection. If port block allocation is enabled (in LSN pool) and a port block size is specified (in the LSN group), the Citrix ADC allocates a random NAT IP address and a block of ports for a subscriber when it initiates a connection for the first time. The ADC allocates this NAT IP address and a port (from the allocated block of ports) for different connections from this subscriber. If all the ports are allocated (for different subscriber's connections) from the subscriber's allocated port block, the ADC allocates a new random port block for the subscriber. Only LSN Pools and LSN groups with the same NAT type settings can be bound together. Multiples LSN pools can be bound to an LSN group. A maximum of 16 LSN pools can be bound to an LSN group.

Possible values: DYNAMIC, DETERMINISTIC Default value: DYNAMIC

portblockallocation Allocate a random NAT port block, from the available NAT port pool of an NAT IP address, for each subscriber when the NAT allocation is set as Dynamic NAT. For any connection initiated from a subscriber, the Citrix ADC allocates a NAT port from the subscriber's allocated NAT port block to create the LSN session.

You must set the port block size in the bound LSN group. For a subscriber, if all the ports are allocated from the subscriber's allocated port block, the Citrix ADC allocates a new random port block for the subscriber.

For Deterministic NAT, this parameter is enabled by default, and you cannot disable it.

Possible values: ENABLED, DISABLED Default value: DISABLED

portrealloctimeout The waiting time, in seconds, between deallocating LSN NAT ports (when an LSN mapping is removed) and reallocating them for a new LSN session. This parameter is necessary in order to prevent collisions between old and new mappings and sessions. It ensures that all established sessions are broken instead of redirected to a different subscriber. This is not applicable for ports used in:

- Deterministic NAT
- Address-Dependent filtering and Address-Port-Dependent filtering
- Dynamic NAT with port block allocation In these cases, ports are immediately reallocated. Default value: 0 Maximum value: 600

maxPortReallocTmq Maximum number of ports for which the port reallocation timeout applies for each NAT IP address. In other words, the maximum deallocated-port queue size for which the reallocation timeout applies for each NAT IP address.

When the queue size is full, the next port deallocated is reallocated immediately for a new LSN session. Default value: 65536 Minimum value: 0 Maximum value: 65536

Example

add lsn pool pool1

rm lsn pool

Remove LSN Pool.

Synopsis

rm lsn pool <poolname>

Arguments

poolname Name for the LSN pool. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN pool is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn pool1" or 'lsn pool1').

Example

rm lsn pool pool1

lsn-rtspalgprofile

The following operations can be performed on "lsn-rtspalgprofile":

add| set| show| rm| unset|

add lsn rtspalgprofile

Add LSN RTSPALG Profile.

Synopsis

add lsn rtspalgprofile <rtspalgprofilename> -rtspportrange <port>

Arguments

rtspalgprofilename The name of the RTSPALG Profile.

rtspIdleTimeout Idle timeout for the rtsp sessions in seconds. Default value: 120 Minimum value: 0

rtspportrange port for the RTSP

rtspTransportProtocol RTSP ALG Profile transport protocol type.

Possible values: TCP, UDP Default value: TCP

Example

add lsn rtspalgprofile profile1

set lsn rtspalgprofile

Set LSN RTSPALG Profile.

Synopsis

set lsn rtspalgprofile <rtspalgprofilename> [-rtspportrange <port>]

Arguments

rtspalgprofilename The name of the RTSPALG Profile.

rtspIdleTimeout Idle timeout for the rtsp sessions in seconds. Default value: 120 Minimum value: 0

rtspportrange port for the RTSP

rtspTransportProtocol RTSP ALG Profile transport protocol type.

Possible values: TCP, UDP Default value: TCP

Example

Set lsn rtspalgprofile profile1

show lsn rtspalgprofile

Display LSN RTSPALG Profile.

Synopsis

show lsn rtspalgprofile

Arguments

rtspalgprofilename The name of the RTSPALG Profile.

Output

rtspIdleTimeout Idle timeout for the rtsp sessions in seconds.

rtspportrange port for the RTSP

rtspTransportProtocol RTSP ALG Profile transport protocol type.

devno count stateflag

Example

show lsn rtspalgprofile profile1

rm lsn rtspalgprofile

Remove LSN RTSPALG Profile.

Synopsis

rm lsn rtspalgprofile <rtspalgprofilename>

Arguments

rtspalgprofilename The name of the RTSPALG Profile.

Example

rm lsn rtspalgprofile profile1

unset lsn rtspalgprofile

Use this command to remove lsn rtspalgprofile settings.Refer to the set lsn rtspalgprofile command for meanings of the arguments.

Synopsis

unset lsn rtspalgprofile <rtspalgprofilename>

lsn-rtspalgsession

The following operations can be performed on "lsn-rtspalgsession":

show| flush|

show lsn rtspalgsession

Show LSN RTSP session.

Synopsis

show lsn rtspalgsession

Arguments

sessionId Session ID for the RTSP call.

Output

callflags Flags for the call entry.

xlatip XLAT IP Address if its XLAT session.

callrefcount Reference count for the call entry.

calltimer Timer for the call entry.

channelip IP address of the channel.

channelnatip Natted IP address of the channel.

channelport port for the channel.

channelnatport Natted port for the channel.

channelprotocol Channel transport protocol.

channelflags Flags for the call entry.

channeltimeout Timeout for the channel.

devno count stateflag

Example

show lsn rtspalgsession

flush lsn rtspalgsession

Flush RTSP session.

Synopsis

flush lsn rtspalgsession <sessionId>

Arguments

sessionId Session ID for the RTSP call.

Example

flush lsn rtspalgsession

lsn-session

The following operations can be performed on "lsn-session":

flush| show|

flush lsn session

Flush LSN Session.

Synopsis

flush lsn session [-nattype <nattype> [-network <ip_addr>]] [-natIP <ip_addr>]

Arguments

nattype Type of sessions to be displayed.

Possible values: NAT44, DS-Lite, NAT64 Default value: NAT44

clientname Name of the LSN Client entity.

network IP address or network address of subscriber(s).

netmask Subnet mask for the IP address specified by the network parameter. Default value: 0xFFFFFFFF

network6 IPv6 address of the LSN subscriber or B4 device.

td Traffic domain ID of the LSN client entity. Default value: 0 Minimum value: 0 Maximum value: 4094

natIP Mapped NAT IP address used in LSN sessions.

natPort Mapped NAT port used in the LSN sessions.

nodeId ID(s) of cluster node(s) on which command is to be executed Default value: -1 Minimum value: 0 Maximum value: 31

Example

flush lsn session

show lsn session

Show LSN Session.

Synopsis

show lsn session [-nattype <nattype> [-network <ip_addr>]]

Arguments

nattype Type of sessions to be displayed.

Possible values: NAT44, DS-Lite, NAT64 Default value: NAT44

clientname Name of the LSN Client entity.

network IP address or network address of subscriber(s).

netmask Subnet mask for the IP address specified by the network parameter. Default value: 0xFFFFFFFF

network6 IPv6 address of the LSN subscriber or B4 device.

td Traffic domain ID of the LSN client entity. Default value: 0 Minimum value: 0 Maximum value: 4094

natIP Mapped NAT IP address used in LSN sessions.

Output

natprefix IPv6 address of the LSN subscriber(s) or subscriber network(B4-Device) on whose traffic the Citrix ADC perform Large Scale NAT.

subscrIP The Source IP address.

subscrPort The Source Port.

destIP The Destination IP address.

destPort The Destination Port.

natPort The NAT Port

transportprotocol The Transport Protocol for the session.

sessionestdir The Session establishment direction, session was established for outbound or inbound packet.

dsttd srctd IPv6Address IPv6 address of v6 vserver

devno count stateflag

Example

show lsn session

lsn-sipalgcall

The following operations can be performed on "lsn-sipalgcall":

flush| show|

flush lsn sipalgcall

Flush LSN Session.

Synopsis

flush lsn sipalgcall <callid>

Arguments

callid Call ID for the SIP call.

Example

flush lsn session

show lsn sipalgcall

Show LSN sipalgcall.

Synopsis

show lsn sipalgcall

Arguments

callid Call ID for the SIP call.

Output

callflags Flags for the call entry.

xlatip XLAT IP Address if its XLAT session.

callrefcount Reference count for the call entry.

calltimer Timer for the call entry.

channelip IP address of the channel.

channelnatip Natted IP address of the channel.

channelport port for the channel.

channelnatport Natted port for the channel.

channelprotocol Channel transport protocol.

channelflags Flags for the call entry.

channeltimeout Timeout for the channel.

devno count stateflag

Example

show lsn sipalgcall

lsn-sipalgprofile

The following operations can be performed on "lsn-sipalgprofile":

set| unset| rm| show| add|

set lsn sipalgprofile

Set LSN SIPALG Profile.

Synopsis

set lsn sipalgprofile <sipalgprofilename> [-sipsrcportrange <port>] [-sipdstportrange <port>]

Arguments

sipalgprofilename The name of the SIPALG Profile.

dataSessionIdleTimeout Idle timeout for the data channel sessions in seconds. Default value: 120 Minimum value: 0

sipSessionTimeout SIP control channel session timeout in seconds. Default value: 600 Minimum value: 0

registrationTimeout SIP registration timeout in seconds. Default value: 60 Minimum value: 0

sipsrcportrange Source port range for SIP_UDP and SIP_TCP.

sipdstportrange Destination port range for SIP_UDP and SIP_TCP.

openRegisterPinhole ENABLE/DISABLE RegisterPinhole creation.

Possible values: ENABLED, DISABLED Default value: ENABLED

openContactPinhole ENABLE/DISABLE ContactPinhole creation.

Possible values: ENABLED, DISABLED Default value: ENABLED

openViaPinhole ENABLE/DISABLE ViaPinhole creation.

Possible values: ENABLED, DISABLED Default value: ENABLED

openRecordRoutePinhole ENABLE/DISABLE RecordRoutePinhole creation.

Possible values: ENABLED, DISABLED Default value: ENABLED

sipTransportProtocol SIP ALG Profile transport protocol type.

Possible values: TCP, UDP

openRoutePinhole ENABLE/DISABLE RoutePinhole creation.

Possible values: ENABLED, DISABLED Default value: ENABLED

rport ENABLE/DISABLE rport.

Possible values: ENABLED, DISABLED Default value: ENABLED

Example

Set lsn sipalgprofile profile1

unset lsn sipalgprofile

Use this command to remove lsn sipalgprofile settings.Refer to the set lsn sipalgprofile command for meanings of the arguments.

Synopsis

unset lsn sipalgprofile <sipalgprofilename>

rm lsn sipalgprofile

Remove LSN SIPALG Profile.

Synopsis

rm lsn sipalgprofile <sipalgprofilename>

Arguments

sipalgprofilename The name of the SIPALG Profile.

Example

rm lsn sipalgprofile profile1

show lsn sipalgprofile

Display LSN SIPALG Profile.

Synopsis

show lsn sipalgprofile

Arguments

sipalgprofilename The name of the SIPALG Profile.

Output

dataSessionIdleTimeout Idle timeout for the data channel sessions in seconds.

sipSessionTimeout SIP control channel session timeout in seconds.

registrationTimeout SIP registration timeout in seconds.

sipsrcportrange Source port range for SIP_UDP and SIP_TCP.

sipdstportrange Destination port range for SIP_UDP and SIP_TCP.

openRegisterPinhole ENABLE/DISABLE RegisterPinhole creation.

openContactPinhole ENABLE/DISABLE ContactPinhole creation.

openViaPinhole ENABLE/DISABLE ViaPinhole creation.

openRecordRoutePinhole ENABLE/DISABLE RecordRoutePinhole creation.

sipTransportProtocol SIP ALG Profile transport protocol type.

openRoutePinhole ENABLE/DISABLE RoutePinhole creation.

rport ENABLE/DISABLE rport.

devno count stateflag

Example

show lsn sipalgprofile profile1

add lsn sipalgprofile

Add LSN SIPALG Profile.

Synopsis

add lsn sipalgprofile <sipalgprofilename> [-sipsrcportrange <port>] [-sipdstportrange <port>] -sipTransportProtocol (TCP | UDP)

Arguments

sipalgprofilename The name of the SIPALG Profile.

dataSessionIdleTimeout Idle timeout for the data channel sessions in seconds. Default value: 120 Minimum value: 0

sipSessionTimeout SIP control channel session timeout in seconds. Default value: 600 Minimum value: 0

registrationTimeout SIP registration timeout in seconds. Default value: 60 Minimum value: 0

sipsrcportrange Source port range for SIP_UDP and SIP_TCP.

sipdstportrange Destination port range for SIP_UDP and SIP_TCP.

openRegisterPinhole ENABLE/DISABLE RegisterPinhole creation.

Possible values: ENABLED, DISABLED Default value: ENABLED

openContactPinhole ENABLE/DISABLE ContactPinhole creation.

Possible values: ENABLED, DISABLED Default value: ENABLED

openViaPinhole ENABLE/DISABLE ViaPinhole creation.

Possible values: ENABLED, DISABLED Default value: ENABLED

openRecordRoutePinhole ENABLE/DISABLE RecordRoutePinhole creation.

Possible values: ENABLED, DISABLED Default value: ENABLED

sipTransportProtocol SIP ALG Profile transport protocol type.

Possible values: TCP, UDP

openRoutePinhole ENABLE/DISABLE RoutePinhole creation.

Possible values: ENABLED, DISABLED Default value: ENABLED

rport ENABLE/DISABLE rport.

Possible values: ENABLED, DISABLED Default value: ENABLED

Example

add lsn sipalgprofile profile1

lsn-static

The following operations can be performed on "lsn-static":

add| show| rm|

add lsn static

Add LSN Static Mapping.

Synopsis

add lsn static <name> <transportprotocol> (<subscrIP>) <subscrPort> [<natIP>] [-destIP <ip_addr>]

Arguments

name Name for the LSN static mapping entry. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn static1" or 'lsn static1').

transportprotocol Protocol for the LSN mapping entry.

Possible values: TCP, UDP, ICMP, ALL

subscrIP IPv4(NAT44 & DS-Lite)/IPv6(NAT64) address of an LSN subscriber for the LSN static mapping entry.

subscrPort Port of the LSN subscriber for the LSN mapping entry. * represents all ports being used. Used in case of static wildcard Maximum value: 65535

network6 B4 address in DS-Lite setup

td ID of the traffic domain to which the subscriber belongs.

If you do not specify an ID, the subscriber is assumed to be a part of the default traffic domain. Default value: 0 Minimum value: 0 Maximum value: 4094

natIP IPv4 address, already existing on the Citrix ADC as type LSN, to be used as NAT IP address for this mapping entry.

natPort NAT port for this LSN mapping entry. * represents all ports being used. Used in case of static wildcard Maximum value: 65535

destIP Destination IP address for the LSN mapping entry.

dsttd ID of the traffic domain through which the destination IP address for this LSN mapping entry is reachable from the Citrix ADC.

If you do not specify an ID, the destination IP address is assumed to be reachable through the default traffic domain, which has an ID of 0. Default value: 0 Minimum value: 0 Maximum value: 4094

Example

add lsn static 10.10.10.100 80

show lsn static

Display LSN Static Mapping.

Synopsis

show lsn static

Arguments

name Name for the LSN static mapping entry. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn static1" or 'lsn static1').

nattype Type of sessions to be displayed.

Possible values: NAT44, DS-Lite, NAT64

Output

transportprotocol Protocol for the LSN mapping entry.

subscrIP IPv4(NAT44 & DS-Lite)/IPv6(NAT64) address of an LSN subscriber for the LSN static mapping entry.

subscrPort Port of the LSN subscriber for the LSN mapping entry. * represents all ports being used. Used in case of static wildcard

network6 B4 address in DS-Lite setup

natIP IPv4 address, already existing on the Citrix ADC as type LSN, to be used as NAT IP address for this mapping entry.

natPort NAT port for this LSN mapping entry. * represents all ports being used. Used in case of static wildcard

td ID of the traffic domain to which the subscriber belongs.

If you do not specify an ID, the subscriber is assumed to be a part of the default traffic domain.

destIP Destination IP address for the LSN mapping entry.

dsttd ID of the traffic domain through which the destination IP address for this LSN mapping entry is reachable from the Citrix ADC.

If you do not specify an ID, the destination IP address is assumed to be reachable through the default traffic domain, which has an ID of 0.

status The status of the Mapping. Status could be Inactive, if mapping addition failed due to already existing dynamic/static mapping, port allocation failure.

devno count stateflag

Example

show lsn static

rm lsn static

Remove LSN Static Mapping.

Synopsis

rm lsn static <name>

Arguments

name Name for the LSN static mapping entry. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the

LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn static1" or 'lsn static1').

Example

rm lsn static

lsn-transportprofile

The following operations can be performed on "lsn-transportprofile":

set| rm| add| unset| show|

set lsn transportprofile

Set LSN Transport Profile.

Synopsis

set lsn transportprofile <transportprofilename>

Arguments

transportprofilename Name for the LSN transport profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN transport profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn transport profile1" or 'lsn transport profile1').

sessiontimeout Timeout, in seconds, for an idle LSN session. If an LSN session is idle for a time that exceeds this value, the Citrix ADC removes the session.

This timeout does not apply for a TCP LSN session when a FIN or RST message is received from either of the endpoints. Default value: 120 Minimum value: 60

finrsttimeout Timeout, in seconds, for a TCP LSN session after a FIN or RST message is received from one of the endpoints.

If a TCP LSN session is idle (after the Citrix ADC receives a FIN or RST message) for a time that exceeds this value, the Citrix ADC ADC removes the session.

Since the LSN feature of the Citrix ADC does not maintain state information of any TCP LSN sessions, this timeout accommodates the transmission of the FIN or RST, and ACK messages from the other endpoint so that both endpoints can properly close the connection. Default value: 30

synidletimeout SYN Idle timeout Default value: 60 Minimum value: 30 Maximum value: 120

portquota Maximum number of LSN NAT ports to be used at a time by each subscriber for the specified protocol. For example, each subscriber can be limited to a maximum of 500 TCP NAT ports. When the LSN NAT mappings for a subscriber reach the limit, the Citrix ADC does not allocate additional NAT ports for that subscriber. Default value: 0 Minimum value: 0 Maximum value: 65535

sessionquota Maximum number of concurrent LSN sessions allowed for each subscriber for the specified protocol. When the number of LSN sessions reaches the limit for a subscriber, the Citrix ADC does not allow the subscriber to open additional sessions. Default value: 0 Minimum value: 0 Maximum value: 65535

groupSessionLimit Maximum number of concurrent LSN sessions(for the specified protocol) allowed for all subscriber of a group to which this profile has bound. This limit will get split across the Citrix ADCs packet engines and rounded down. When the number of LSN sessions reaches the limit for a group in packet engine, the Citrix ADC does not allow the subscriber of that group to open additional sessions through that packet engine. Default value: 0 Minimum value: 0

portpreserveparity Enable port parity between a subscriber port and its mapped LSN NAT port. For example, if a subscriber initiates a connection from an odd numbered port, the Citrix ADC allocates an odd numbered LSN NAT port for this connection. You must set this parameter for proper functioning of protocols that require the source port to be even or odd numbered, for example, in peer-to-peer applications that use RTP or RTCP protocol.

Possible values: ENABLED, DISABLED Default value: DISABLED

portpreserverange If a subscriber initiates a connection from a well-known port (0-1023), allocate a NAT port from the well-known port range (0-1023) for this connection. For example, if a subscriber initiates a connection from port 80, the Citrix ADC can allocate port 100 as the NAT port for this connection.

This parameter applies to dynamic NAT without port block allocation. It also applies to Deterministic NAT if the range of ports allocated includes well-known ports.

When all the well-known ports of all the available NAT IP addresses are used in different subscriber's connections (LSN sessions), and a subscriber initiates a connection from a well-known port, the Citrix ADC drops this connection.

Possible values: ENABLED, DISABLED Default value: DISABLED

syncheck Silently drop any non-SYN packets for connections for which there is no LSN-NAT session present on the Citrix ADC.

If you disable this parameter, the Citrix ADC accepts any non-SYN packets and creates a new LSN session entry for this connection.

Following are some reasons for the Citrix ADC to receive such packets:

- LSN session for a connection existed but the Citrix ADC removed this session because the LSN session was idle for a time that exceeded the configured session timeout.
- Such packets can be a part of a DoS attack.

Possible values: ENABLED, DISABLED Default value: ENABLED

Example

set lsn transportprofile profile1 -portquota 128

rm lsn transportprofile

Remove LSN Transport Profile.

Synopsis

rm lsn transportprofile <transportprofilename>

Arguments

transportprofilename Name for the LSN transport profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN transport profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn transport profile1" or 'lsn transport profile1').

Example

rm lsn transportprofile profile1

add lsn transportprofile

Add LSN Transport Profile.

Synopsis

add lsn transportprofile <transportprofilename> <transportprotocol>

Arguments

transportprofilename Name for the LSN transport profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN transport profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn transport profile1" or 'lsn transport profile1').

transportprotocol Protocol for which to set the LSN transport profile parameters.

Possible values: TCP, UDP, ICMP

sessiontimeout Timeout, in seconds, for an idle LSN session. If an LSN session is idle for a time that exceeds this value, the Citrix ADC removes the session.

This timeout does not apply for a TCP LSN session when a FIN or RST message is received from either of the endpoints. Default value: 120 Minimum value: 60

finrsttimeout Timeout, in seconds, for a TCP LSN session after a FIN or RST message is received from one of the endpoints.

If a TCP LSN session is idle (after the Citrix ADC receives a FIN or RST message) for a time that exceeds this value, the Citrix ADC ADC removes the session.

Since the LSN feature of the Citrix ADC does not maintain state information of any TCP LSN sessions, this timeout accommodates the transmission of the FIN or RST, and ACK messages from the other endpoint so that both endpoints can properly close the connection. Default value: 30

synidletimeout SYN Idle timeout Default value: 60 Minimum value: 30 Maximum value: 120

portquota Maximum number of LSN NAT ports to be used at a time by each subscriber for the specified protocol. For example, each subscriber can be limited to a maximum of 500 TCP NAT ports. When the LSN NAT mappings for a subscriber reach the limit, the Citrix ADC does not

allocate additional NAT ports for that subscriber. Default value: 0 Minimum value: 0 Maximum value: 65535

sessionquota Maximum number of concurrent LSN sessions allowed for each subscriber for the specified protocol. When the number of LSN sessions reaches the limit for a subscriber, the Citrix ADC does not allow the subscriber to open additional sessions. Default value: 0 Minimum value: 0 Maximum value: 65535

groupSessionLimit Maximum number of concurrent LSN sessions(for the specified protocol) allowed for all subscriber of a group to which this profile has bound. This limit will get split across the Citrix ADCs packet engines and rounded down. When the number of LSN sessions reaches the limit for a group in packet engine, the Citrix ADC does not allow the subscriber of that group to open additional sessions through that packet engine. Default value: 0 Minimum value: 0

portpreserveparity Enable port parity between a subscriber port and its mapped LSN NAT port. For example, if a subscriber initiates a connection from an odd numbered port, the Citrix ADC allocates an odd numbered LSN NAT port for this connection. You must set this parameter for proper functioning of protocols that require the source port to be even or odd numbered, for example, in peer-to-peer applications that use RTP or RTCP protocol.

Possible values: ENABLED, DISABLED Default value: DISABLED

portpreserverange If a subscriber initiates a connection from a well-known port (0-1023), allocate a NAT port from the well-known port range (0-1023) for this connection. For example, if a subscriber initiates a connection from port 80, the Citrix ADC can allocate port 100 as the NAT port for this connection.

This parameter applies to dynamic NAT without port block allocation. It also applies to Deterministic NAT if the range of ports allocated includes well-known ports.

When all the well-known ports of all the available NAT IP addresses are used in different subscriber's connections (LSN sessions), and a subscriber initiates a connection from a well-known port, the Citrix ADC drops this connection.

Possible values: ENABLED, DISABLED Default value: DISABLED

syncheck Silently drop any non-SYN packets for connections for which there is no LSN-NAT session present on the Citrix ADC.

If you disable this parameter, the Citrix ADC accepts any non-SYN packets and creates a new LSN session entry for this connection.

Following are some reasons for the Citrix ADC to receive such packets:

- LSN session for a connection existed but the Citrix ADC removed this session because the LSN session was idle for a time that exceeded the configured session timeout.
- Such packets can be a part of a DoS attack.

Possible values: ENABLED, DISABLED Default value: ENABLED

Example

add lsn transportprofile profile1 TCP -portquota 128

unset lsn transportprofile

Use this command to remove lsn transportprofile settings.Refer to the set lsn transportprofile command for meanings of the arguments.

Synopsis

unset lsn transportprofile <transportprofilename>

show lsn transportprofile

Display LSN Transport Profile.

Synopsis

show lsn transportprofile

Arguments

transportprofilename Name for the LSN transport profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN transport profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn transport profile1" or 'lsn transport profile1').

Output

transportprotocol Protocol for which to set the LSN transport profile parameters.

sessiontimeout Timeout, in seconds, for an idle LSN session. If an LSN session is idle for a time that exceeds this value, the Citrix ADC removes the session.

This timeout does not apply for a TCP LSN session when a FIN or RST message is received from either of the endpoints.

finrsttimeout Timeout, in seconds, for a TCP LSN session after a FIN or RST message is received from one of the endpoints.

If a TCP LSN session is idle (after the Citrix ADC receives a FIN or RST message) for a time that exceeds this value, the Citrix ADC ADC removes the session.

Since the LSN feature of the Citrix ADC does not maintain state information of any TCP LSN sessions, this timeout accommodates the transmission of the FIN or RST, and ACK messages from the other endpoint so that both endpoints can properly close the connection.

stuntimeout STUN protocol timeout

synidletimeout SYN Idle timeout

portquota Maximum number of LSN NAT ports to be used at a time by each subscriber for the specified protocol. For example, each subscriber can be limited to a maximum of 500 TCP NAT ports. When the LSN NAT mappings for a subscriber reach the limit, the Citrix ADC does not allocate additional NAT ports for that subscriber.

sessionquota Maximum number of concurrent LSN sessions allowed for each subscriber for the specified protocol. When the number of LSN sessions reaches the limit for a subscriber, the Citrix ADC does not allow the subscriber to open additional sessions.

groupSessionLimit Maximum number of concurrent LSN sessions(for the specified protocol) allowed for all subscriber of a group to which this profile has bound. This limit will get split across the Citrix ADCs packet engines and rounded down. When the number of LSN sessions reaches the limit for a group in packet engine, the Citrix ADC does not allow the subscriber of that group to open additional sessions through that packet engine.

portpreserveparity Enable port parity between a subscriber port and its mapped LSN NAT port. For example, if a subscriber initiates a connection from an odd numbered port, the Citrix ADC allocates an odd numbered LSN NAT port for this connection. You must set this parameter for proper functioning of protocols that require the source port to be even or odd numbered, for example, in peer-to-peer applications that use RTP or RTCP protocol.

portpreserverange If a subscriber initiates a connection from a well-known port (0-1023), allocate a NAT port from the well-known port range (0-1023) for this connection. For example, if a

subscriber initiates a connection from port 80, the Citrix ADC can allocate port 100 as the NAT port for this connection.

This parameter applies to dynamic NAT without port block allocation. It also applies to Deterministic NAT if the range of ports allocated includes well-known ports.

When all the well-known ports of all the available NAT IP addresses are used in different subscriber's connections (LSN sessions), and a subscriber initiates a connection from a well-known port, the Citrix ADC drops this connection.

syncheck Silently drop any non-SYN packets for connections for which there is no LSN-NAT session present on the Citrix ADC.

If you disable this parameter, the Citrix ADC accepts any non-SYN packets and creates a new LSN session entry for this connection.

Following are some reasons for the Citrix ADC to receive such packets:

- LSN session for a connection existed but the Citrix ADC removed this session because the LSN session was idle for a time that exceeded the configured session timeout.
- Such packets can be a part of a DoS attack.

devno count stateflag

Example

show lsn transportprofile profile1

lsn

The following operations can be performed on "lsn":

stat lsn

Display Large Scale NAT statistics.

Synopsis

stat lsn

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

LSN TCP Received Packets (TcpRxPkts) Number of LSN TCP Received packets.

LSN TCP Received Bytes (TcpRxBytes) Number of LSN TCP Received bytes.

LSN TCP Transmitted Packets (TcpTxPkts) Number of LSN TCP Transmitted packets.

LSN TCP Transmitted Bytes (TcpTxBytes) Number of LSN TCP Transmitted bytes.

LSN TCP Dropped Packets (TcpDrpPkts) Number of LSN TCP Dropped packets.

LSN TCP Current Sessions (TcpSess) Number of LSN TCP Current Sessions.

LSN UDP Received Packets (UdpRxPkts) Number of LSN UDP Received packets.

LSN UDP Received Bytes (UdpRxBytes) Number of LSN UDP Received bytes.

LSN UDP Transmitted Packets (UdpTxPkts) Number of LSN UDP Transmitted packets.

LSN UDP Transmitted Bytes (UdpTxBytes) Number of LSN UDP Transmitted bytes.

LSN UDP Dropped Packets (UdpDrpPkts) Number of LSN UDP Dropped packets.

LSN UDP Current Sessions (UdpSess) Number of LSN UDP Current Sessions.

LSN ICMP Received Packets (IcmpRxPkts) Number of LSN ICMP Received packets.

LSN ICMP Received Bytes (IcmpRxBytes) Number of LSN ICMP Received bytes.

LSN ICMP Transmitted Packets (IcmpTxPkts) Number of LSN ICMP Transmitted packets.

LSN ICMP Transmitted Bytes (IcmpTxBytes) Number of LSN ICMP Transmitted bytes.

LSN ICMP Dropped Packets (IcmpDrpPkts) Number of LSN ICMP Dropped packets.

LSN ICMP Current Sessions (IcmpSess) Number of LSN ICMP Current Sessions.

LSN sessions (Session) Current number of LSN sessions.

LSN Subscribers (Subscr) Current number of LSN subscribers.

Related Commands

- stat lsn nat64

network

L2Param

The following operations can be performed on "L2Param":

set| unset| show|

set L2Param

Set Layer 2 related global settings on the Citrix ADC

Synopsis

set L2Param

Arguments

mbfPeermacUpdate When mbf_instant_learning is enabled, learn any changes in peer's MAC after this time interval, which is in 10ms ticks. Default value: 10 Minimum value: 0

maxBridgeCollision Maximum bridge collision for loop detection Default value: 20 Minimum value: 0

bdggrpProxyArp Set/reset proxy ARP in bridge group deployment

Possible values: ENABLED, DISABLED Default value: ENABLED

bdgSetting Bridging settings for C2C behavior. If enabled, each PE will learn MAC entries independently. Otherwise, when L2 mode is ON, learned MAC entries on a PE will be broadcasted to all other PEs.

Possible values: ENABLED, DISABLED Default value: DISABLED

garpOnVridIntf Send GARP messagess on VRID-configured interfaces upon failover

Possible values: ENABLED, DISABLED Default value: ENABLED

macModeFwdMyPkt Allows MAC mode vserver to pick and forward the packets even if it is destined to Citrix ADC owned VIP.

Possible values: ENABLED, DISABLED Default value: DISABLED

useMyMAC Use Citrix ADC MAC for all outgoing packets.

Possible values: ENABLED, DISABLED Default value: DISABLED

proxyArp Proxies the ARP as Citrix ADC MAC for FreeBSD.

Possible values: ENABLED, DISABLED Default value: ENABLED

garpReply Set/reset REPLY form of GARP

Possible values: ENABLED, DISABLED Default value: DISABLED

mbfInstLearning Enable instant learning of MAC changes in MBF mode.

Possible values: ENABLED, DISABLED Default value: DISABLED

rstIntfOnHaFo Enable the reset interface upon HA failover.

Possible values: ENABLED, DISABLED Default value: DISABLED

skipProxyingBsdTraffic Control source parameters (IP and Port) for FreeBSD initiated traffic. If Enabled, source parameters are retained. Else proxy the source parameters based on next hop.

Possible values: ENABLED, DISABLED Default value: DISABLED

returnToEthernetSender Return to ethernet sender.

Possible values: ENABLED, DISABLED Default value: DISABLED

stopMacMoveUpdate Stop Update of server mac change to NAT sessions.

Possible values: ENABLED, DISABLED Default value: DISABLED

bridgeAgeTimeout Time-out value for the bridge table entries, in seconds. The new value applies only to the entries that are dynamically learned after the new value is set. Previously existing bridge table entries expire after the previously configured time-out value. Default value: 300 Minimum value: 60 Maximum value: 300

useNetprofileBSDTraffic Control source parameters (IP and Port) for FreeBSD initiated traffic. If enabled proxy the source parameters based on netprofile source ip. If netprofile does not have ip configured, then it will continue to use NSIP as earlier.

Possible values: ENABLED, DISABLED Default value: DISABLED

Related Commands

- show l2param

unset L2Param

Use this command to remove L2Param settings.Refer to the set L2Param command for meanings of the arguments.

Synopsis

unset L2Param

show L2Param

Displays the settings of global Layer 2 parameters on the Citrix ADC.

Synopsis

show L2Param

Arguments

Output

maxBridgeCollision Maximum bridge collision for loop detection

linkMTU this MTU is used for Ready logo purpose, changing the Interface MTU at soft layer level.

mbfPeermacUpdate When mbf_instant_learning is enabled, learn any changes in peer's MAC after this time interval, which is in 10ms ticks.

bdggrpProxyArp Set/reset proxy ARP in bridge group deployment

bdgSetting Bridging settings for C2C behavior. If enabled, each PE will learn MAC entries independently. Otherwise, when L2 mode is ON, learned MAC entries on a PE will be broadcasted to all other PEs.

garpOnVridIntf Send GARP messagess on VRID-configured interfaces upon failover

macModeFwdMyPkt Allows MAC mode vserver to pick and forward the packets even if it is destined to Citrix ADC owned VIP.

useMyMAC Use Citrix ADC MAC for all outgoing packets.

proxyArp Proxies the ARP as Citrix ADC MAC for FreeBSD.

garpReply Set/reset REPLY form of GARP

mbfInstLearning Enable instant learning of MAC changes in MBF mode.

rstIntfOnHaFo Enable the reset interface upon HA failover.

skipProxyingBsdTraffic Control source parameters (IP and Port) for FreeBSD initiated traffic. If Enabled, source parameters are retained. Else proxy the source parameters based on next hop.

returnToEthernetSender Return to ethernet sender.

stopMacMoveUpdate Stop Update of server mac change to NAT sessions.

bridgeAgeTimeout Time-out value for the bridge table entries, in seconds. The new value applies only to the entries that are dynamically learned after the new value is set. Previously existing bridge table entries expire after the previously configured time-out value.

useNetprofileBSDTraffic Control source parameters (IP and Port) for FreeBSD initiated traffic. If enabled proxy the source parameters based on netprofile source ip. If netprofile does not have ip configured, then it will continue to use NSIP as earlier.

Related Commands

- show l2param

L3Param

The following operations can be performed on "L3Param":

unset| set| show|

unset L3Param

Use this command to remove L3Param settings.Refer to the set L3Param command for meanings of the arguments.

Synopsis

unset L3Param

set L3Param

Set Layer 3 related global settings on the Citrix ADC

Synopsis

set L3Param

Arguments

srcnat Perform NAT if only the source is in the private network

Possible values: ENABLED, DISABLED Default value: ENABLED

icmpGenRateThreshold NS generated ICMP pkts per 10ms rate threshold Default value: 100 Minimum value: 0

overrideRnat USNIP/USIP settings override RNAT settings for configured service/virtual server traffic..

Possible values: ENABLED, DISABLED Default value: DISABLED

dropDFFlag Enable dropping the IP DF flag.

Possible values: ENABLED, DISABLED Default value: DISABLED

mipRoundRobin Enable round robin usage of mapped IPs.

Possible values: ENABLED, DISABLED Default value: ENABLED

externalLoopBack Enable external loopback.

Possible values: ENABLED, DISABLED Default value: DISABLED

tnlPmtuWoConn Enable/Disable learning PMTU of IP tunnel when ICMP error does not contain connection information.

Possible values: ENABLED, DISABLED Default value: ENABLED

usipServerStrayPkt Enable detection of stray server side pkts in USIP mode.

Possible values: ENABLED, DISABLED Default value: DISABLED

forwardICMPFragments Enable forwarding of ICMP fragments.

Possible values: ENABLED, DISABLED Default value: DISABLED

dropIPFragments Enable dropping of IP fragments.

Possible values: ENABLED, DISABLED Default value: DISABLED

AclLogTime Parameter to tune acl logging time Default value: 5000 Minimum value: 0

implicitACLAllow Do not apply ACLs for internal ports

Possible values: ENABLED, DISABLED Default value: ENABLED

dynamicRouting Enable/Disable Dynamic routing on partition. This configuration is not applicable to default partition

Possible values: ENABLED, DISABLED Default value: DISABLED

ipv6DynamicRouting Enable/Disable IPv6 Dynamic routing

Possible values: ENABLED, DISABLED Default value: DISABLED

allowClassEIPv4 Enable/Disable IPv4 Class E address clients

Possible values: ENABLED, DISABLED Default value: DISABLED

Related Commands

- show l3param

show L3Param

Displays the settings of global Layer 3 parameters.

Synopsis

show L3Param

Arguments

Output

srcnat Perform NAT if only the source is in the private network

icmpGenRateThreshold NS generated ICMP pkts per 10ms rate threshold

overrideRnat USNIP/USIP settings override RNAT settings for configured service/virtual server traffic..

dropDFFlag Enable dropping the IP DF flag.

mipRoundRobin Enable round robin usage of mapped IPs.

externalLoopBack Enable external loopback.

tnlPmtuWoConn Enable/Disable learning PMTU of IP tunnel when ICMP error does not contain connection information.

usipServerStrayPkt Enable detection of stray server side pkts in USIP mode.

forwardICMPFragments Enable forwarding of ICMP fragments.

dropIPFragments Enable dropping of IP fragments.

AclLogTime Parameter to tune acl logging time

implicitACLAllow Do not apply ACLs for internal ports

dynamicRouting Enable/Disable Dynamic routing on partition. This configuration is not applicable to default partition

ipv6DynamicRouting Enable/Disable IPv6 Dynamic routing

allowClassEIPv4 Enable/Disable IPv4 Class E address clients

Related Commands

- show l3param

L4Param

The following operations can be performed on "L4Param":

unset| set| show|

unset L4Param

Use this command to remove L4Param settings.Refer to the set L4Param command for meanings of the arguments.

Synopsis

unset L4Param

set L4Param

Set Layer 4 related global settings on the Citrix ADC

Synopsis

set L4Param

Arguments

l2ConnMethod Layer 2 connection method based on the combination of channel number, MAC address and VLAN. It is tuned with l2conn param of lb vserver. If l2conn of lb vserver is ON then method specified here will be used to identify a connection in addition to the 4-tuple (<source IP>:<source port>::<destination IP>:<destination port>).

Possible values: Channel, Vlan, VlanChannel, Mac, MacChannel, MacVlan, MacVlanChannel Default value: MacVlanChannel

l4switch In L4 switch topology, always clients and servers are on the same side. Enable l4switch to allow such connections.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set l4param

Related Commands

- show l4param

show L4Param

Displays the settings of global Layer 4 parameters.

Synopsis

show L4Param

Arguments

Output

l2ConnMethod Layer 2 connection method based on the combination of channel number, MAC address and VLAN. It is tuned with l2conn param of lb vserver. If l2conn of lb vserver is ON then method specified here will be used to identify a connection in addition to the 4-tuple (<source IP>:<source port>::<destination IP>:<destination port>).

l4switch In L4 switch topology, always clients and servers are on the same side. Enable l4switch to allow such connections.

Related Commands

- unset l4param

MapBmr

The following operations can be performed on "MapBmr":

add| show| unbind| stat| bind| rm|

add MapBmr

Add MAP-T Basic Mapping rule.

Synopsis

add MapBmr <name> -RuleIpv6Prefix <ipv6_addr|*>

Arguments

name Name for the Basic Mapping Rule. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the MAP Basic Mapping Rule is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "add network MapBmr bmr1 -natprefix 2005::/64 -EAbitLength 16 -psidoffset 6 -portsharingratio 8"). The Basic Mapping Rule information allows a MAP BR to determine source IPv4 address from the IPv6 packet sent from MAP CE device. Also it allows to determine destination IPv6 address of MAP CE before sending packets to MAP CE

RuleIpv6Prefix IPv6 prefix of Customer Edge(CE) device.MAP-T CE will send ipv6 packets with this ipv6 prefix as source ipv6 address prefix

psidoffset Start bit position of Port Set Identifier(PSID) value in Embedded Address (EA) bits. Default value: 6 Minimum value: 1 Maximum value: 15

EAbitLength The Embedded Address (EA) bit field encodes the CE-specific IPv4 address and port information. The EA bit field, which is unique for a given Rule IPv6 prefix. Default value: 16 Minimum value: 2 Maximum value: 47

psidlength Length of Port Set IdentifierPort Set Identifier(PSID) in Embedded Address (EA) bits Default value: 8 Minimum value: 1 Maximum value: 16

Example

add network MapBmr bmr1 -natprefix 2005::/64 -EAbitLength 16 -psidoffset 6 -portsharingratio 8

show MapBmr

Display Basic mapping rule.

Synopsis

show MapBmr

Arguments

name Name for the Basic Mapping Rule. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the MAP Basic Mapping Rule is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "add network MapBmr bmr1 -natprefix 2005::/64 -EAbitLength 16 -psidoffset 6 -portsharingratio 8"). The Basic Mapping Rule information allows a MAP BR to determine source IPv4 address from the IPv6 packet sent from MAP CE device. Also it allows to determine destination IPv6 address of MAP CE before sending packets to MAP CE

Output

RuleIpv6Prefix IPv6 prefix of Customer Edge(CE) device.MAP-T CE will send ipv6 packets with this ipv6 prefix as source ipv6 address prefix

network IPv4 NAT address range of Customer Edge (CE).

netmask Subnet mask for the IPv4 address specified in the Network parameter.

EAbitLength The Embedded Address (EA) bit field encodes the CE-specific IPv4 address and port information. The EA bit field, which is unique for a given Rule IPv6 prefix.

psidoffset Start bit position of Port Set Identifier(PSID) value in Embedded Address (EA) bits.

psidlength Length of Port Set IdentifierPort Set Identifier(PSID) in Embedded Address (EA) bits

devno count stateflag

Example

show network MapBmr bmr1

unbind MapBmr

unbind network from BMR rule.

Synopsis

unbind MapBmr <name> (-network <ip_addr>)

Arguments

name Name for the Basic Mapping Rule. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the MAP Basic Mapping Rule is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "add network MapBmr bmr1 -natprefix 2005::/64 -EAbitLength 16 -psidoffset 6 -portsharingratio 8"). The Basic Mapping Rule information allows a MAP BR to determine source IPv4 address from the IPv6 packet sent from MAP CE device. Also it allows to determine destination IPv6 address of MAP CE before sending packets to MAP CE

network IPv4 NAT address range of Customer Edge (CE).

netmask Subnet mask for the IPv4 address specified in the Network parameter. Default value: 0xFFFFFFFF

Example

unbind network MapBmr bmr1 -network 192.168.0.0 -netmask 255.255.255.0

stat MapBmr

Display MAP Basic Mapping Rule statistics.

Synopsis

stat MapBmr

Arguments

name Basic Mapping Rule name.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

MAP-T BMR IPv6 Rx packets (v6rxPkts) Total number of MAP-T BMR V6 Recieved packets.

MAP-T BMR IPv6 Tx packets (v6txPkts) Total number of MAP-T BMR V6 Transmitted packets.

MAP-T BMR IPv4 Rx packets (v4rxPkts) Total number of MAP-T BMR V4 Recieved packets.

MAP-T BMR IPv4 Tx packets (v4txPkts) Total number of MAP-T BMR V4 Transmitted packets.

MAP-T BMR IPv6 TCP Rx packets (v6rxPktsTcp) Total number of MAP-T BMR V6 TCP Recieved packets.

MAP-T BMR IPv6 TCP Tx packets (v6txPktsTcp) Total number of MAP-T BMR V6 TCP Transmitted packets.

MAP-T BMR IPv4 TCP Rx packets (v4rxPktsTcp) Total number of MAP-T BMR V4 TCP Recieved packets.

MAP-T BMR IPv4 TCP Tx packets (v4txBytesTcp) Total number of MAP-T BMR V4 TCP Transmitted packets.

MAP-T BMR IPv6 UDP Rx packets (v6rxPktsUdp) Total number of MAP-T BMR V6 UDP Recieved packets.

MAP-T BMR IPv6 UDP Tx packets (v6txPktsUdp) Total number of MAP-T BMR V6 UDP Transmitted packets.

MAP-T BMR IPv4 UDP Rx packets (v4rxPktsUdp) Total number of MAP-T BMR V4 UDP Recieved packets.

MAP-T BMR IPv4 UDP Tx packets (v4txBytesUdp) Total number of MAP-T BMR V4 UDP Transmitted packets.

MAP-T BMR IPv6 ICMP Rx packets (v6rxPktsIcmp) Total number of MAP-T BMR V6 ICMP Recieved packets.

MAP-T BMR IPv6 ICMP Tx packets (v6txPktsIcmp) Total number of MAP-T BMR V6 ICMP Transmitted packets.

MAP-T BMR IPv4 ICMP Rx packets (v4rxPktsIcmp) Total number of MAP-T BMR V4 ICMP Recieved packets.

MAP-T BMR IPv4 ICMP Tx packets (v4txBytesIcmp) Total number of MAP-T BMR V4 ICMP Transmitted packets.

Example

stat mapbmr

Related Commands

- stat MapDomain

bind MapBmr

Bind network to BMR rule.

Synopsis

bind MapBmr <name> (-network <ip_addr>)

Arguments

name Name for the Basic Mapping Rule. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the MAP Basic Mapping Rule is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example,

"add network MapBmr bmr1 -natprefix 2005::/64 -EAbitLength 16 -psidoffset 6 -portsharingratio 8"). The Basic Mapping Rule information allows a MAP BR to determine source IPv4 address from the IPv6 packet sent from MAP CE device. Also it allows to determine destination IPv6 address of MAP CE before sending packets to MAP CE

network IPv4 NAT address range of Customer Edge (CE).

netmask Subnet mask for the IPv4 address specified in the Network parameter. Default value: 0xFFFFFFFF

Example

bind network MapBmr bmr1 -network 192.168.0.0 -netmask 255.255.255.0

rm MapBmr

Remove MAP Basic Mapping Rule.

Synopsis

rm MapBmr <name>

Arguments

name Name for the Basic Mapping Rule. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the MAP Basic Mapping Rule is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "add network MapBmr bmr1 -natprefix 2005::/64 -EAbitLength 16 -psidoffset 6 -portsharingratio 8"). The Basic Mapping Rule information allows a MAP BR to determine source IPv4 address from the IPv6 packet sent from MAP CE device. Also it allows to determine destination IPv6 address of MAP CE before sending packets to MAP CE

Example

rm network MapBmr bmr1

MapDmr

The following operations can be performed on "MapDmr":

rm| show| add|

rm MapDmr

Remove MAP-T Default Mapping rule.

Synopsis

rm MapDmr <name>

Arguments

name Name for the Default Mapping Rule. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the MAP Default Mapping Rule is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "add network MapDmr map1 -BRIpv6Prefix 2003::/96"). Default Mapping Rule (DMR) is defined in terms of the IPv6 prefix advertised by one or more BRs, which provide external connectivity. A typical MAP-T CE will install an IPv4 default route using this rule. A BR will use this rule when translating all outside IPv4 source addresses to the IPv6 MAP domain.

Example

rm network MapDmr map1

show MapDmr

Display MAP-T Default Mapping rule.

Synopsis

show MapDmr

Arguments

name Name for the Default Mapping Rule. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the MAP Default Mapping Rule is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "add network MapDmr map1 -BRIpv6Prefix 2003::/96"). Default Mapping Rule (DMR) is defined in terms of the IPv6 prefix advertised by one or more BRs, which provide external connectivity. A typical MAP-T CE will install an IPv4 default route using this rule. A BR will use this rule when translating all outside IPv4 source addresses to the IPv6 MAP domain.

Output

BRIpv6Prefix IPv6 prefix of Border Relay (Citrix ADC) device.MAP-T CE will send ipv6 packets to this ipv6 prefix.The DMR IPv6 prefix length SHOULD be 64 bits long by default and in any case MUST NOT exceed 96 bits

devno count stateflag

Example

show network MapDmr map1

add MapDmr

Add MAP-T Default Mapping rule.

Synopsis

add MapDmr <name> -BRIpv6Prefix <ipv6_addr|*>

Arguments

name Name for the Default Mapping Rule. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the MAP Default Mapping Rule is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "add network MapDmr map1 -BRIpv6Prefix 2003::/96"). Default Mapping Rule (DMR) is defined in terms of the IPv6 prefix advertised by one or more BRs, which provide external connectivity. A typical MAP-T CE will install an IPv4 default route using this rule. A BR will use this rule when translating all outside IPv4 source addresses to the IPv6 MAP domain.

BRIpv6Prefix IPv6 prefix of Border Relay (Citrix ADC) device.MAP-T CE will send ipv6 packets to this ipv6 prefix.The DMR IPv6 prefix length SHOULD be 64 bits long by default and in any case MUST NOT exceed 96 bits

Example

add network MapDmr map1 -BRIpv6Prefix 2003::/96

MapDomain

The following operations can be performed on "MapDomain":

unbind| add| bind| show| rm| stat|

unbind MapDomain

unbind MAP Domain from BMR rule.

Synopsis

unbind MapDomain <name> -MapBmrName <string>

Arguments

name Name for the MAP Domain. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the MAP Domain is created . The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "add network MapDomain map1").

MapBmrName Basic Mapping rule name.

Example

unbind network MapDomain map1 -MapBmrName bmr1

add MapDomain

Add MAP Domain.

Synopsis

add MapDomain <name> -MapDmrName <string>

Arguments

name Name for the MAP Domain. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the MAP Domain is created . The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "add network MapDomain map1").

MapDmrName Default Mapping rule name.

Example

add network MapDomain map1 -MapBmrName dmr1

bind MapDomain

Bind MAP domain with BMR rule.

Synopsis

bind MapDomain <name> -MapBmrName <string>

Arguments

name Name for the MAP Domain. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the MAP Domain is created . The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "add network MapDomain map1").

MapBmrName Basic Mapping rule name.

Example

bind network MapDomain map1 -MapBmrName bmr1

show MapDomain

Display MAP Domain.

Synopsis

show MapDomain

Arguments

name Name for the MAP Domain. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the MAP Domain is created . The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "add network MapDomain map1").

Output

MapDmrName Default Mapping rule name.

MapBmrName Basic Mapping rule name.

devno count stateflag

Example

show network MapDomain map1

rm MapDomain

Remove MAP Domain.

Synopsis

rm MapDomain <name>

Arguments

name Name for the MAP Domain. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the MAP Domain is created . The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "add network MapDomain map1").

Example

rm network MapDomain map1

stat MapDomain

Display MAP Domain statistics.

Synopsis

stat MapDomain

Arguments

name An integer specifying the VLAN identification number (VID). Possible values: 1 through 4094.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

MAP-T IPv6 TCP Rx packets (v6rxPktsTcp) Total number of MAP-T IPv6 TCP Recieved packets.

MAP-T IPv6 TCP Tx packets (v6txPktsTcp) Total number of MAP-T IPv6 TCP Transmitted packets.

MAP-T IPv6 TCP Rx Bytes (v6rxBytesTcp) Total number of MAP-T IPv6 TCP Recieved Bytes.

MAP-T IPv6 TCP Tx Bytes (v6txBytesTcp) Total number of MAP-T IPv6 TCP Transmitted Bytes.

MAP-T IPv4 TCP Rx packets (v4rxPktsTcp) Total number of MAP-T IPv4 TCP Recieved packets.

MAP-T IPv4 TCP Tx packets (v4txPktsTcp) Total number of MAP-T IPv4 TCP Transmitted packets.

MAP-T IPv4 TCP Rx Bytes (v4rxBytesTcp) Total number of MAP-T IPv4 TCP Recieved Bytes.

MAP-T IPv4 TCP Tx Bytes (v4txBytesTcp) Total number of MAP-T IPv4 TCP Transmitted Bytes.

MAP-T IPv6 UDP Rx packets (v6rxPktsUdp) Total number of MAP-T IPv6 UDP Recieved packets.

MAP-T IPv6 UDP Tx packets (v6txPktsUdp) Total number of MAP-T IPv6 UDP Transmitted packets.

MAP-T IPv6 UDP Rx Bytes (v6rxBytesUdp) Total number of MAP-T IPv6 UDP Recieved Bytes.

MAP-T IPv6 UDP Tx Bytes (v6txBytesUdp) Total number of MAP-T IPv6 UDP Transmitted Bytes.

MAP-T IPv4 UDP Rx packets (v4rxPktsUdp) Total number of MAP-T IPv4 UDP Recieved packets.

MAP-T IPv4 UDP Tx packets (v4txPktsUdp) Total number of MAP-T IPv4 UDP Transmitted packets.

MAP-T IPv4 UDP Rx Bytes (v4rxBytesUdp) Total number of MAP-T IPv4 UDP Recieved Bytes.

MAP-T IPv4 UDP Tx Bytes (v4txBytesUdp) Total number of MAP-T IPv4 UDP Transmitted Bytes.

MAP-T IPv6 ICMP Rx packets (v6rxPktsIcmp) Total number of MAP-T IPv6 ICMP Recieved packets.

MAP-T IPv6 ICMP Tx packets (v6txPktsIcmp) Total number of MAP-T IPv6 ICMP Transmitted packets.

MAP-T IPv6 ICMP Rx Bytes (v6rxBytesIcmp) Total number of MAP-T IPv6 ICMP Recieved Bytes.

MAP-T IPv6 ICMP Tx Bytes (v6txBytesIcmp) Total number of MAP-T IPv6 ICMP Transmitted Bytes.

MAP-T IPv4 ICMP Rx packets (v4rxPktsIcmp) Total number of MAP-T IPv4 ICMP Recieved packets.

MAP-T IPv4 ICMP Tx packets (v4txPktsIcmp) Total number of MAP-T IPv4 ICMP Transmitted packets.

MAP-T IPv4 ICMP Rx Bytes (v4rxBytesIcmp) Total number of MAP-T IPv4 ICMP Recieved Bytes.

MAP-T IPv4 ICMP Tx Bytes (v4txBytesIcmp) Total number of MAP-T IPv4 ICMP Transmitted Bytes.

MAP-T Total V6 Recieved packets (v6rxPkts) Total number of MAP-T V6 Recieved packets.

MAP-T Total V6 Transmitted packets (v6txPkts) Total number of MAP-T V6 Transmitted packets.

MAP-T Total V4 Recieved packets (v4rxPkts) Total number of MAP-T V4 Recieved packets.

MAP-T Total V4 Transmitted packets (v4txPkts) Total number of MAP-T V4 Transmitted packets.

Example

stat mapdomain

Related Commands

- stat MapBmr

appAlgParam

The following operations can be performed on "appAlgParam":

show| set| unset|

show appAlgParam

Display the global parameters for APP ALG

Synopsis

show appAlgParam

Arguments

Output

pptpGreIdleTimeout Interval in sec, after which data sessions of PPTP GRE is cleared.

Example

show appalgparam

set appAlgParam

Sets the global parameters for APP ALG

Synopsis

set appAlgParam -pptpGreIdleTimeout <positive_integer>

Arguments

pptpGreIdleTimeout Interval in sec, after which data sessions of PPTP GRE is cleared. Default value: 9000 Minimum value: 1 Maximum value: 9000

Example

set appalgparam -pptpGreIdleTimeout 15000

unset appAlgParam

Use this command to remove appAlgParam settings.Refer to the set appAlgParam command for meanings of the arguments.

Synopsis

unset appAlgParam -pptpGreIdleTimeout

arp

The following operations can be performed on "arp":

send| rm| show| add|

send arp

Sends Gratuitous Address Resolution Protocol (GARP) messages for the specified Citrix ADC owned IP addresses.

Synopsis

send arp ((-IPAddress <ip_addr>) | -all)

Arguments

IPAddress Citrix ADC owned IP address for which the Citrix ADC sends Gratuitous Address Resolution Protocol (GARP) messages.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

all Send GARP messages for all Citrix ADC owned IP addresses on which the ARP option is enabled. In a secondary node of an high availability configuration, this option sends GARP messages for the node's NSIP address only.

Example

send arp 10.10.10.10

rm arp

Removes a specified static ARP entry or all static ARP entries from the Citrix ADC's ARP table.

Synopsis

rm arp (<IPAddress> | -all)

Arguments

IPAddress IP address of the network device in the ARP entry that you want to remove from the ARP table.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

all Remove all ARP entries from the ARP table of the Citrix ADC.

ownerNode The owner node for the Arp entry. Default value: -1 Minimum value: 0 Maximum value: 31

show arp

Display all the entries in the system's ARP table.

Synopsis

show arp [<IPAddress>]

Arguments

IPAddress The IP address corresponding to an ARP entry.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

ownerNode The cluster node which owns the ARP entry. Default value: -1 Minimum value: 0 Maximum value: 31

Output

mac The MAC address corresponding to an ARP entry.

ifnum The interface on which this MAC address resides.

timeout The time, in seconds, after which the entry times out.

state The state of the ARP entry.

flags The flags for the entry.

type Indicates whether this ARP entry was added manually or dynamically. When you manually add an ARP entry, the value for this parameter is STATIC. Otherwise, it is DYNAMIC. For the NSIP and loopback IP addresses, the value is PERMANENT.

vlan The VLAN ID through which packets are to be sent after matching the ARP entry. This is a numeric value.

vxlan ID of the VXLAN on which the IP address of this ARP entry is reachable.

vtep IP address of the VXLAN tunnel endpoint (VTEP) through which the IP address of this ARP entry is reachable.

channel The tunnel, channel, or physical interface through which the ARP entry is identified.

flag Flags for the entry.

controlPlane This arp entry is populated by a control plane protocol

devno count stateflag

Example

The output of the sh arp command is as follows: 5 configured arps: IP MAC Inface VLAN Origin TTL Traffic Domain

1. 10.250.11.1 00:04:76:dc:f1:b9 1/2 2 dynamic 700 0
2. 10.11.0.254 00:30:19:c1:7e:f4 1/1 1 dynamic 500 0
3. 10.11.0.41 00:d0:a8:00:7c:e4 0/1 1 dynamic 500 0
4. 10.11.222.2 00:ee:ff:22:00:01 0/1 1 dynamic 500 0
5. 10.11.201.12 00:30:48:31:23:49 0/1 1 dynamic 500 0

add arp

Adds a static ARP entry to the ARP table of the Citrix ADC.

Synopsis

add arp -IPAddress <ip_addr> -mac <mac_addr> (-ifnum <interface_name> | -vxlan <positive_integer>)

Arguments

IPAddress IP address of the network device that you want to add to the ARP table.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

mac MAC address of the network device.

ifnum Interface through which the network device is accessible. Specify the interface in (slot/port) notation. For example, 1/3.

vxlan ID of the VXLAN on which the IP address of this ARP entry is reachable. Minimum value: 1 Maximum value: 16777215

vtep IP address of the VXLAN tunnel endpoint (VTEP) through which the IP address of this ARP entry is reachable.

vlan The VLAN ID through which packets are to be sent after matching the ARP entry. This is a numeric value. Minimum value: 0

ownerNode The owner node for the Arp entry. Default value: -1 Minimum value: 0 Maximum value: 31

Example

add arp -ip 10.100.0.48 -mac 00:a0:cc:5f:76:3a -ifnum 1/1

arpparam

The following operations can be performed on "arpparam":

unset| set| show|

unset arpparam

Use this command to remove arpparam settings.Refer to the set arpparam command for meanings of the arguments.

Synopsis

unset arpparam

set arpparam

Sets a global time-out value for dynamic ARP entries.

Synopsis

set arpparam

Arguments

timeout Time-out value (aging time) for the dynamically learned ARP entries, in seconds. The new value applies only to ARP entries that are dynamically learned after the new value is set. Previously existing ARP entries expire after the previously configured aging time. Default value: 1200 Minimum value: 5 Maximum value: 1200

spoofValidation enable/disable arp spoofing validation

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set arpparam -timeout 200 -spoofvalidate ENABLE

show arpparam

Display the global setting of dynamically learned ARP entries.

Synopsis

show arpparam

Arguments

Output

timeout The ARP table entry aging time, in seconds.

spoofValidation enable/disable arp spoofing validation

Example

show arpparam

bridge

The following operations can be performed on "bridge":

stat bridge

Display bridging statistics.

Synopsis

stat bridge

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Loops The number of times bridging registered MAC moved

Collisions (Collisns) The number of bridging table collisions

Interface muted (Mutes) The number of bridging related interface mutes

Total bridged packets (Tot_pkts) The total number of bridged packets

Total bridged Mbits (Tot_Mbits) The total number of bridged Mbits

Related Commands

- stat MapDomain

bridgegroup

The following operations can be performed on "bridgegroup":

bind| unbind| show| unset| add| set| rm|

bind bridgegroup

Bind a vlan or an ip address to a bridgegroup.

Synopsis

bind bridgegroup <id> [-IPAddress <ip_addr|ipv6_addr|*>]

Arguments

id The integer that uniquely identifies the bridge group. Minimum value: 1 Maximum value: 1000

vlan An integer that uniquely identifies the VLAN that you want to bind to this bridge group. Minimum value: 2 Maximum value: 4094

IPAddress A network address or addresses to be associated with the bridge group. You must add entries for these network addresses in the routing table before running this command.

netmask A subnet mask associated with the network address.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

ownerGroup The owner node group in a Cluster for this vlan. Default value: DEFAULT_NG

Example

bind bridgegroup 1 -vlan 2

unbind bridgegroup

Unbinds the specified VLANs or IP addresses from a bridge group.

Synopsis

unbind bridgegroup <id> [-IPAddress <ip_addr|ipv6_addr|*>]

Arguments

id Integer that uniquely identifies the bridge group. Minimum value: 1 Maximum value: 1000

vlan ID of the VLAN to unbind from this bridge group. Minimum value: 2 Maximum value: 4094

IPAddress Network address associated with the bridge group.

netmask The network mask for the subnet defined for the bridge group.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

ownerGroup The owner node group in a Cluster for this vlan. Default value: DEFAULT_NG

show bridgegroup

Display the configured bridge group. If a name is specified, only that particular bridge group information is displayed. Otherwise, all configured bridge groups are displayed.

Synopsis

show bridgegroup

Arguments

id The name of the bridge group. Minimum value: 1 Maximum value: 1000

Output

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

IPAddress The IP address assigned to the bridge group.

netmask The network mask for the subnet defined for the bridge group.

flags Temporary flag used for internal purpose.

portbitmap Member interfaces of this bridge group.

tagbitmap Tagged members of this bridge group.

ifaces Names of all member interfaces of this bridge group.

tagIfaces Names of all tagged member interfaces of this bridge group.

vlan Names of all member VLANs.

dynamicRouting Whether dynamic routing is enabled or disabled.

ipv6DynamicRouting Whether ipv6 dynamic routing is enabled or disabled.

rnat Temporary flag used for internal purpose.

flag partitionName Name of the Partition to which this vlan bound to.

ownerGroup The owner node group in a Cluster for this vlan.

devno count stateflag

Example

An example of the output of the show bridge group command is as follows: 2 configured Bridge Group: 1)

```
    Bridge Group: 1

    Member vlans : 2 3 4
```

IP: 10.102.33.27 MASK: 255.255.255.0 2) Bridge Group: 2 Member vlans : 5 6

unset bridgegroup

Use this command to remove bridgegroup settings.Refer to the set bridgegroup command for meanings of the arguments.

Synopsis

unset bridgegroup <id>

add bridgegroup

Create a Bridge group.

Synopsis

add bridgegroup <id>

Arguments

id An integer that uniquely identifies the bridge group. Minimum value: 1 Maximum value: 1000

dynamicRouting Enable dynamic routing for this bridgegroup.

Possible values: ENABLED, DISABLED Default value: DISABLED

ipv6DynamicRouting Enable all IPv6 dynamic routing protocols on all VLANs bound to this bridgegroup. Note: For the ENABLED setting to work, you must configure IPv6 dynamic routing protocols from the VTYSH command line.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

add bridgegroup 1

set bridgegroup

Set Bridge group parameters.

Synopsis

set bridgegroup <id>

Arguments

id An integer value that uniquely identifies the bridge group. Minimum value: 1. Maximum value: 1000. Minimum value: 1 Maximum value: 1000

dynamicRouting Enable dynamic routing for this bridgegroup.

Possible values: ENABLED, DISABLED Default value: DISABLED

ipv6DynamicRouting Enable all IPv6 dynamic routing protocols on this bridge group. For this setting to work, you must configure IPv6 dynamic routing protocols from the VTYSH command line. For more information about configuring IPv6 dynamic routing protocols on the Citrix ADC, see the Dynamic Routing chapter of the Citrix ADC Networking Guide.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set bridgegroup 1 -dynamicRouting ENABLED

rm bridgegroup

Remove the bridge group created by the add bridge group command.

Synopsis

rm bridgegroup <id>

Arguments

id An integer that uniquely identifies the bridge group that you want to remove from the Citrix ADC. Minimum value: 1 Maximum value: 1000

bridgetable

The following operations can be performed on "bridgetable":

show| add| unset| clear| rm| set|

show bridgetable

Displays the bridge table entries and the configured time-out values for these entries.

Synopsis

show bridgetable

Arguments

Output

bridgeAge Time-out value for the bridge table entries, in seconds. The new value applies only to the entries that are dynamically learned after the new value is set. Previously existing bridge table entries expire after the previously configured time-out value.

mac The MAC address of the target.

ifnum The interface on which the address was learned.

vlan The VLAN in which this MAC address resides.

vxlan The VXLAN in which this MAC address resides.

vtep The IP address of the destination VXLAN tunnel endpoint where the Ethernet MAC ADDRESS resides.

vni The VXLAN VNI Network Identifier (or VXLAN Segment ID) to use to connect to the remote VXLAN tunnel endpoint. If omitted the value specified as vxlan will be used.

deviceVlan The vlan on which to send multicast packets when the VXLAN tunnel endpoint is a muticast group address.

flags Display flags,

type Whether static or dynamic

channel The Tunnel through which bridge entry is learned.

controlPlane This bridge table entry is populated by a control plane protocol

devno count stateflag

Example

show bridgetable

add bridgetable

Add static mac-vtep mappings per vxlan

Synopsis

add bridgetable -mac <mac_addr> -vxlan <positive_integer> -vtep <ip_addr>

Arguments

mac The MAC address of the target.

vxlan The VXLAN to which this address is associated. Minimum value: 1 Maximum value: 16777215

vtep The IP address of the destination VXLAN tunnel endpoint where the Ethernet MAC ADDRESS resides.

vni The VXLAN VNI Network Identifier (or VXLAN Segment ID) to use to connect to the remote VXLAN tunnel endpoint. If omitted the value specified as vxlan will be used. Minimum value: 1 Maximum value: 16777215

deviceVlan The vlan on which to send multicast packets when the VXLAN tunnel endpoint is a muticast group address. Minimum value: 1 Maximum value: 4094

Example

add bridgetable -mac 52:f2:46:e6:ed:67 -vxlan 100 -vtep 172.16.1.24 add bridgetable -mac c2:76:29:4a:fe:9e -vxlan 100 -vtep 192.168.7.1 -vni 200 add bridgetable -mac 00:00:00:00:00:00

-vxlan 100 -vtep 172.16.1.24 add bridgetable -mac 00:00:00:00:00:00 -vxlan 100 -vtep 239.0.0.1 -deviceVlan 23 add bridgetable -mac 00:00:00:00:00:00 -vxlan 100 -vtep 239.0.0.1 -deviceVlan 24

unset bridgetable

Use this command to remove bridgetable settings.Refer to the set bridgetable command for meanings of the arguments.

Synopsis

unset bridgetable

clear bridgetable

Remove entries from bridge table

Synopsis

clear bridgetable

Arguments

vlan VLAN whose entries are to be removed. Minimum value: 1 Maximum value: 4094

ifnum INTERFACE whose entries are to be removed.

vxlan VXLAN whose entries are to be removed. Minimum value: 1 Maximum value: 16777215

rm bridgetable

Delete static mac-vtep mapping

Synopsis

rm bridgetable -mac <mac_addr> -vxlan <positive_integer>

Arguments

mac The MAC address of the target.

vxlan The VXLAN to which this address is associated. Minimum value: 1 Maximum value: 16777215

vtep The IP address of the destination VXLAN tunnel endpoint where the Ethernet MAC ADDRESS resides.

deviceVlan The vlan on which to send multicast packets when the VXLAN tunnel endpoint is a muticast group address. Minimum value: 1 Maximum value: 4094

Example

rm bridgetable -mac 52:f2:46:e6:ed:67 -vxlan 100 rm bridgetable -mac 00:00:00:00:00:00 -vxlan 100 -vtep 172.16.1.24 rm bridgetable -mac 00:00:00:00:00:00 -vxlan 100 -vtep 239.0.0.1 -deviceVlan 23

set bridgetable

Sets global parameters of bridge table entries. The bridgeAge attribute is deprecated. Use "set l2param -bridgeAgeTimeout" instead.

Synopsis

set bridgetable

Arguments

Example

set bridgetable -bridgeAge 200

channel

The following operations can be performed on "channel":

add| bind| rm| unbind| show| set| unset|

add channel

Creates a link aggregate channel on the Citrix ADC or on a cluster configuration. Link aggregation combines data coming from multiple ports into a single high-speed link. Configuring link aggregation increases the capacity and availability of the communication channel between the Citrix ADC appliance and other connected devices. When a network interface is bound to a channel, the channel parameters have precedence over the network interface parameters. That is, the network interface parameters are ignored. A network interface can be bound only to one channel.

Synopsis

add channel <id> [-bandwidthHigh <positive_integer>]

Arguments

id ID for the LA channel or cluster LA channel or LR channel to be created. Specify an LA channel in LA/x notation, where x can range from 1 to 8 or cluster LA channel in CLA/x notation or Link redundant channel in LR/x notation, where x can range from 1 to 4. Cannot be changed after the LA channel is created.

ifnum Interfaces to be bound to the LA channel of a Citrix ADC or to the LA channel of a cluster configuration. For an LA channel of a Citrix ADC, specify an interface in C/U notation (for example, 1/3). For an LA channel of a cluster configuration, specify an interface in N/C/U notation (for example, 2/1/3). where C can take one of the following values:

- 0 - Indicates a management interface.
- 1 - Indicates a 1 Gbps port.
- 10 - Indicates a 10 Gbps port. U is a unique integer for representing an interface in a particular port group. N is the ID of the node to which an interface belongs in a cluster configuration. Use spaces to separate multiple entries.

state Enable or disable the LA channel.

Possible values: ENABLED, DISABLED Default value: ENABLED

lamac Specifies a MAC address for the LA channels configured in Citrix ADC virtual appliances (VPX). This MAC address is persistent after each reboot. If you don't specify this parameter, a MAC address is generated randomly for each LA channel. These MAC addresses change after each reboot.

speed Ethernet speed of the channel, in Mbps. If the speed of any bound interface is greater than or equal to the value set for this parameter, the state of the interface is UP. Otherwise, the state is INACTIVE. Bound Interfaces whose state is INACTIVE do not process any traffic.

Possible values: AUTO, 10, 100, 1000, 10000, 25000, 40000, 50000, 100000 Default value: AUTO

flowControl Specifies the flow control type for this LA channel to manage the flow of frames. Flow control is a function as mentioned in clause 31 of the IEEE 802.3 standard. Flow control allows congested ports to pause traffic from the peer device. Flow control is achieved by sending PAUSE frames.

Possible values: OFF, RX, TX, RXTX, ON Default value: OFF

haMonitor In a High Availability (HA) configuration, monitor the LA channel for failure events. Failure of any LA channel that has HA MON enabled triggers HA failover.

Possible values: ON, OFF Default value: ON

haHeartbeat In a High Availability (HA) configuration, configure the LA channel for sending heartbeats. LA channel that has HA Heartbeat disabled should not send the heartbeats.

Possible values: OFF, ON Default value: ON

tagall Adds a four-byte 802.1q tag to every packet sent on this channel. The ON setting applies tags for all VLANs that are bound to this channel. OFF applies the tag for all VLANs other than the native VLAN.

Possible values: ON, OFF Default value: OFF

ifAlias Alias name for the LA channel. Used only to enhance readability. To perform any operations, you have to specify the LA channel ID. Default value: " "

throughput Low threshold value for the throughput of the LA channel, in Mbps. In an high availability (HA) configuration, failover is triggered when the LA channel has HA MON enabled and the throughput is below the specified threshold. Minimum value: 0 Maximum value: 160000

bandwidthHigh High threshold value for the bandwidth usage of the LA channel, in Mbps. The Citrix ADC generates an SNMP trap message when the bandwidth usage of the LA channel is greater than or equal to the specified high threshold value. Minimum value: 0 Maximum value: 160000

bandwidthNormal Normal threshold value for the bandwidth usage of the LA channel, in Mbps. When the bandwidth usage of the LA channel returns to less than or equal to the specified normal threshold after exceeding the high threshold, the Citrix ADC generates an SNMP trap message to indicate that the bandwidth usage has returned to normal. Minimum value: 0 Maximum value: 160000

bind channel

Binds the specified interfaces to a channel.

Synopsis

bind channel <id> <ifnum> ...

Arguments

id ID of the LA channel or the cluster LA channel to which you want to bind interfaces. Specify an LA channel in LA/x notation, where x can range from 1 to 8 or a cluster LA channel in CLA/x notation or Link redundant channel in LR/x notation , where x can range from 1 to 4.

ifnum Interfaces to be bound to the LA channel of a Citrix ADC or to the LA channel of a cluster configuration.

In case of standalone or HA configuration, Maximum 16 interfaces can be bound to a channel. In case of Cluster configuration, Maximum 16 interfaces can be bound to a Node level channel and maximum 16 interafce from each node can be bound to a Cluster level channel.

For an LA channel of a Citrix ADC, specify an interface in C/U notation (for example, 1/3). For an LA channel of a cluster configuration, specify an interface in N/C/U notation (for example, 2/1/3). where C can take one of the following values:

- 0 - Indicates a management interface.
- 1 - Indicates a 1 Gbps port.
- 10 - Indicates a 10 Gbps port.
- 40 - Indicates a 40 Gbps port. U is a unique integer for representing an interface in a particular port group. N is the ID of the node to which an interface belongs in a cluster configuration. Use spaces to separate multiple entries.

rm channel

Removes an LA channel from the Citrix ADC or a cluster LA channel from a cluster configuration. Important: When a LA channel is removed, the network interfaces bound to it induce network loops that decrease network performance. You must disable the network interfaces before you remove the channel.

Synopsis

rm channel <id>

Arguments

id ID of the LA channel or cluster LA channel or Link Redundant channel that you want to remove. Specify an LA channel in LA/x notation, where x can range from 1 to 8 or a cluster LA channel in CLA/x notation or Link redundant channel in LR/x notation , where x can range from 1 to 4.

unbind channel

Unbinds the specified interfaces from an LA channel.

Synopsis

unbind channel <id> <ifnum> ...

Arguments

id ID of the LA channel or cluster LA channel from which you want to unbind interfaces. Specify an LA channel in LA/x notation, where x can range from 1 to 8 or a cluster LA channel in CLA/x notation or Link redundant channel in LR/x notation , where x can range from 1 to 4.

ifnum Interfaces to be unbound from the LA channel of a Citrix ADC or from the LA channel of a cluster configuration. For an LA channel of a Citrix ADC, specify an interface in C/U notation (for example, 1/3). For an LA channel of a cluster configuration, specify an interface in N/C/U notation (for example, 2/1/3). where C can take one of the following values:

- 0 - Indicates a management interface.
- 1 - Indicates a 1 Gbps port.
- 10 - Indicates a 10 Gbps port. U is a unique integer for representing an interface in a particular port group. N is the ID of the node to which an interface belongs in a cluster configuration. Use spaces to separate multiple entries.

show channel

Displays the settings of all LA channels or of the specified channel. To display the settings of all channels, run the command without any parameters. To display the settings of a particular channel, specify the ID of the channel.

Synopsis

show channel

Arguments

id ID of an LA channel or LA channel in cluster configuration whose details you want the Citrix ADC to display. Specify an LA channel in LA/x notation, where x can range from 1 to 8 or a cluster LA channel in CLA/x notation or Link redundant channel in LR/x notation , where x can range from 1 to 4. Minimum value: 1

Output

stateflag deviceName LA channel name in form LA/x, where x is channel ID, which ranges from 1 to 8 or LR channel name in form LR/x, where x is channel ID, which ranges from 1 to 4

unit Unit number of the channel. This is an internal reference number that the Citrix ADC uses to identify the channel.

description The IEEE standard that the channel is based on.

flags Flags of this channel.

mtu The Maximum Transmission Unit (MTU) is the largest packet size, measured in bytes excluding 14 bytes ethernet header and 4 bytes CRC, that can be transmitted and received by an interface. The default value of MTU is 1500 on all the interface of Citrix ADC, some Cloud Platforms will restrict Citrix ADC to use the lesser default value. Any MTU value more than 1500 is called Jumbo MTU and will make the interface as jumbo enabled. The Maximum Jumbo MTU in Citrix ADC is 9216, however, some Virtualized / Cloud Platforms will have lesser Maximum Jumbo MTU Value (9000). In the case of Cluster, the Backplane interface requires an MTU value of 78 bytes more than the Max MTU configured on any other Data-Plane Interface. When the Data plane interfaces are all at default 1500 MTU, Cluster Back Plane will be automatically set to 1578 (1500 + 78) MTU. If a Backplane interface is reset to Data Plane Interface, then the 1578 MTU will be automatically reset to the default MTU of 1500(or whatever lesser default value). If any data plane interface of a Cluster is configured with a Jumbo MTU (> 1500), then all backplane interfaces require to be configured with a minimum MTU of 'Highest Data Plane MTU in the Cluster + 78'. That makes the maximum Jumbo MTU for any Data-Plane Interface in a Cluster System to be '9138 (9216 - 78)., where 9216 is the maximum Jumbo MTU. On certain Virtualized / Cloud Platforms, the maximum possible MTU is restricted to a lesser value, Similar calculation can be applied, Maximum Data Plane MTU in Cluster = (Maximum possible MTU - 78).

actualMtu MTU of the channel. This is the maximum frame size that the channel can process.

vlan Native VLAN of the channel.

mac MAC address of the channel.

lamac Specifies a MAC address for the LA channels configured in Citrix ADC virtual appliances (VPX). This MAC address is persistent after each reboot. If you don't specify this parameter, a MAC address is generated randomly for each LA channel. These MAC addresses change after each reboot.

uptime Duration for which the channel is UP. (Example: 3 hours 1 minute 1 second). This value is reset when the channel state changes to DOWN.

downTime Duration for which the channel is DOWN. (Example: 3 hours 1 minute 1 second). This value is reset when the channel state changes to UP.

reqMedia Requested media setting for this channel. Since there is no media associated with LA, the displayed values carry no significance.

reqSpeed Requested speed setting for this channel. Since no media are associated with LA, this speed is used to determine the threshold for the slave interfaces. If the speed of the member interface is less than the requested speed, that interface is considered inactive.

reqDuplex Requested duplex setting for this channel. Since no media are associated with LA, the displayed values carry no significance.

reqFlowcontrol Requested flow control setting for this channel. Since no media are associated with LA, the displayed values carry no significance.

media Actual media setting for this channel.

speed Ethernet speed of the channel, in Mbps. If the speed of any bound interface is greater than or equal to the value set for this parameter, the state of the interface is UP. Otherwise, the state is INACTIVE. Bound Interfaces whose state is INACTIVE do not process any traffic.

duplex Actual duplex setting for this channel.

flowControl Specifies the flow control type for this LA channel to manage the flow of frames. Flow control is a function as mentioned in clause 31 of the IEEE 802.3 standard. Flow control allows congested ports to pause traffic from the peer device. Flow control is achieved by sending PAUSE frames.

media Requested media setting for this interface.

speed Actual speed setting for this channel.

duplex Actualduplex setting for this interface.

flowControl Actual flow control setting for this channel.

Mode The type of LA: static LA or dynamic LA (LACP). Possible values: Manual, AUTO. Manual shows the static LA, and AUTO shows the LACP.

Mode The mode(AUTO/MANNUAL) for the LA channel.

haMonitor HA monitoring enabled or disabled for this channel.

haHeartbeat The state of HA HEARTBEAT SEND for the LA channel.

state Enable or disable the LA channel.

autoneg Requested auto negotiation setting for this channel. Since no media are associated with LA, this setting has no effect.

autonegResult Actual auto negotiation setting for this channel.

tagged VLAN tags setting on this channel.

tagall The appliance adds a four-byte 802.1q tag to every packet sent on this channel. ON applies tags for all the VLANs that are bound to this channel. OFF, applies the tag for all VLANs other than the native VLAN.

trunk This is deprecated by tagall

taggedAny Channel setting to accept/drop all tagged packets.

taggedAutolearn Dynaminc vlan membership on this channel.

hangDetect Hang detect for this channel.

hangReset Hang reset for this channel.

linkState The current state of the link associated with the interface. For logical interfaces (LA), the state of the link is dependent on the state of the slave interfaces. For the link to be UP at least one of the slave interfaces needs to be UP.

intfState Current state of the specified interface. The interface state set to UP only if the link state is UP and administrative state is ENABLED.

rxpackets Number of bytes received by all the slave interfaces of the channel since the Citrix ADC was started or the interface statistics were cleared.

rxbytes Number of packets received by all member interfaces since the Citrix ADC was started or the interface statistics were cleared.

rxerrors Number of inbound packets dropped by the hardware of the slave interfaces since the Citrix ADC was started or the interface statistics were cleared. Possible causes of dropped packets are CRC, length (undersize or oversize), and alignment errors.

rxdrops Number of inbound packets dropped by the channel's slave interfaces. Commonly dropped packets are multicast frames, spanning tree BPDUs, packets destined to a MAC not owned by the Citrix ADC when L2 mode is disabled, or packets tagged for a VLAN that is not bound to the interface. In most healthy networks, this statistic increments at a steady rate regardless of traffic load. A sharp spike in dropped packets generally indicates an issue with connected L2 switches, such as a forwarding database overflow resulting in packets being broadcast on all ports.

txpackets Number of packets transmitted by slave interfaces of a channel since the Citrix ADC was started or the interface statistics were cleared.

txbytes Number of bytes transmitted by slave interfaces of a channel since the Citrix ADC was started or the interface statistics were cleared.

txerrors Number of outbound packets dropped by the hardware of a channel's slave interfaces since the Citrix ADC was started or the interface statistics were cleared. Possible causes of dropped packets are length (undersize or oversize) errors and lack of resources.

txdrops Number of packets dropped in transmission by a channel's slave interfaces for one of the following reasons: (1) VLAN mismatch. (2) Oversized packets. (3) Interface congestion. (4) Loopback packets sent on non-loopback interface.

inDisc Number of error-free inbound packets discarded by a channel's slave interfaces because of a lack of resources (for example, insufficient receive buffers).

outDisc Number of error-free outbound packets discarded by a channel's slave interfaces because of a lack of resources. This statistic is not available on: (1) 10G ports of Citrix ADC MPX 12500/12500/15500-10G platforms. (2) 10G data ports on Citrix ADC MPX 17500/19500/21500 platforms.

fctls Number of times flow control is performed on a channel's slave interfaces because of pause frames.

hangs Number of hangs that occurred on the channel's slave interfaces.

stsStalls Number of status stalls that occurred on the channel's slave interfaces.

txStalls Number of Tx stalls happened that occurred on the channel's slave interfaces.

rxStalls Number of Rx stalls that occurred on the channel's slave interfaces.

bdgMuted Number of times a channel's slave interfaces stopped transmitting and receiving packets because of MAC moves between ports.

vmac Virtual MAC of this channel.

vmac6 Virtual MAC for IPv6 on this interface.

ifAlias The alias name for the interface.

reqThroughput Minimum required throughput for an interface. Failover is triggered if the operating throughput of a Link Aggregation (LA) channel for which HAMON is ON falls below this value.

lrMinThroughput Specifies the minimum throughput threshold (in Mbps) to be met by the active subchannel. Setting this parameter automatically divides an LACP channel into logical subchannels, with one subchannel active and the others in standby mode. When the maximum supported throughput of the active channel falls below the lrMinThroughput value, link failover occurs and a standby subchannel becomes active.

linkRedundancy Link Redundancy for Cluster LAG.

throughput Low threshold value for the throughput of the LA channel, in Mbps. In an high availability (HA) configuration, failover is triggered when the LA channel has HA MON enabled and the throughput is below the specified threshold.

throughput Actual throughput for the interface.

bandwidthHigh High threshold value for the bandwidth usage of the LA channel, in Mbps. The Citrix ADC generates an SNMP trap message when the bandwidth usage of the LA channel is greater than or equal to the specified high threshold value.

bandwidthNormal Normal threshold value for the bandwidth usage of the LA channel, in Mbps. When the bandwidth usage of the LA channel returns to less than or equal to the specified normal threshold after exceeding the high threshold, the Citrix ADC generates an SNMP trap message to indicate that the bandwidth usage has returned to normal.

ifnum The interfaces bound to link aggregate channel.

backplane The cluster backplane status of the LA. If the status is enabled, the LA is part of the cluster backplane. By default, the backplane status is disabled.

clearTime Time since the interface stats are cleared last time.

slavestate State of the member interfaces.

slavemedia Media type of the member interfaces.

slavespeed Speed of the member interfaces.

slaveduplex Duplex of the member interfaces.

slaveflowctl Flowcontrol of the member interfaces.

slavetime UP time of the member interfaces.

lacpMode The LACP mode of the specified interface. The possible values are:

1. Active: A port in active mode generates LACP protocol messages on a regular basis, regardless of any need expressed by its partner to receive them.
2. Passive: A port in passive mode generally does not transmit LACP messages unless its partner is in the active mode; that is, it does not speak unless spoken to.
3. Disabled: Removes the interface from the LA channel. If this is only interface in the LA channel, the LA channel is also deleted.

lacpTimeout Time to wait for the LACPDU. If a LACPDU is not received within this interval, the Citrix ADC markes the link partner port as DOWN. Possible values: Long and Short. Long lacptimeout is 90 sec and Short LACP timeout is 3 sec.

lacpActorPriority LACP Actor Priority. A LACP port priority is configured on each port using LACP. LACP uses the port priority with the port number to form the port identifier. The port priority determines which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

lacpActorPortno LACP Actor port number. LACP uses the port priority with the port number to form the port identifier.

lacpPartnerState LACP Partner State. Whether the port is in Active or Passive negotiating state.

lacpPartnerTimeout The timeout value for the information revieved in LACPDUs. It can have values as SHORT or LONG. The SHORT timeout is 3s and the LONG timeout is 90s.

lacpPartnerAggregation The Aggregation flag indicates that the participant will allow the link to be used as part of an aggregate. Otherwise the link is to be used as an individual link, i.e. not aggregated with any other.

lacpPartnerInsync The Synchronization flag indicates that the transmitting participant.s mux component is in sync with the system id and key information transmitted.

lacpPartnerCollecting The Collecting flag indicates that the participant.s collector, i.e. the reception component of the mux, is definitely on. If set the flag communicates collecting.

lacpPartnerDistributing The Distributing flag indicates that the participant.s distributor is not definitely off. If reset the flag indicates not distributing.

lacpPartnerDefaulted If the timer expires in the Expired state, the Receive Machine enters the Defaulted state.

lacpPartnerExpired If the LACPDUs are received for timeout period, the Receive Machine enters the Expired state and the timer is restarted with the timeout value of SHORT timeout

lacpPartnerPriority LACP Partner Priority. A LACP port priority is configured on each port using LACP. LACP uses the port priority with the port number to form the port identifier. The port priority determines which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

lacpPartnerSystemMac LACP Partner System MAC.

lacpPartnerSystemPriority LACP Partner System Priority. The LACP partner's system priority. The values for the priority range from 0 to 65535. The lower the value, the higher the system priority. The switch with the lower system priority value determines which links between LACP partner are active and which are in the standby for each LACP Channel.

lacpPartnerPortno LACP Partner Port number. LACP uses the port priority with the port number to form the port identifier.

lacpPartnerKey LACP Partner Key. The LACP key used by the partner port.

lacpActorAggregation The Aggregation flag indicates that the participant will allow the link to be used as part of an aggregate. Otherwise the link is to be used as an individual link, i.e. not aggregated with any other.

lacpActorInsync The Synchronization flag indicates that the transmitting participant.s mux component is in sync with the system id and key information transmitted.

lacpActorCollecting The Collecting flag indicates that the participant.s collector, i.e. the reception component of the mux, is definitely on. If set the flag communicates collecting.

lacpActorDistributing The Distributing flag indicates that the participant.s distributor is not definitely off. If reset the flag indicates not distributing.

lacpPortMuxState LACP Port MUX state. The state of the MUX control machine. The Mux Control Machine attaches the physical port to an aggregate port, using the Selection Logic to choose an appropriate port, and turns the distributor and collector for the physical port on or off as required by protocolinformation.

lacpPortRxStat LACP Port RX state. The state of the Receive machine. The Receive Machine maintains partner information, recording protocol information from LACPDUs sent by remote partner(s). Received information is subject to a timeout, and if sufficient time elapses the receive machine will revert to using default partner information.

lacpPortSelectState LACP Port SELECT state. The state of the SELECT state machine, It could be SELECTED or UNSELECTED.

lldpmode Link Layer Discovery Protocol (LLDP) mode for an interface. The resultant LLDP mode of an interface depends on the LLDP mode configured at the global and the interface levels.

svmCmd New attribute added to identify the source of cmd, when SVM fires the nitro cmd, it will set the value of SVMCMD to be 1.

lrActiveIntf LR set member interface state(active/inactive).

devno count

set channel

Modifies the specified parameters of an LA channel.

Synopsis

set channel <id> [-bandwidthHigh <positive_integer>]

Arguments

id ID of the LA channel or the cluster LA channel whose parameters you want to modify. Specify an LA channel in LA/x notation, where x can range from 1 to 8 or a cluster LA channel in CLA/x notation or Link redundant channel in LR/x notation , where x can range from 1 to 4. Required for identifying the LA channel and cannot be modified.

state Enable or disable the LA channel.

Possible values: ENABLED, DISABLED Default value: ENABLED

lamac Allows User to set MAC address for LA channels on Hypervised platforms.

speed The speed for the LA channel.

Possible values: AUTO, 10, 100, 1000, 10000, 25000, 40000, 50000, 100000 Default value: AUTO

mtu The Maximum Transmission Unit (MTU) is the largest packet size, measured in bytes excluding 14 bytes ethernet header and 4 bytes CRC, that can be transmitted and received by an interface. The default value of MTU is 1500 on all the interface of Citrix ADC, some Cloud Platforms will restrict Citrix ADC to use the lesser default value. Any MTU value more than 1500 is called Jumbo MTU and will make the interface as jumbo enabled. The Maximum Jumbo MTU in Citrix ADC is 9216, however, some Virtualized / Cloud Platforms will have lesser Maximum Jumbo MTU Value (9000). In the case of Cluster, the Backplane interface requires an MTU value of 78 bytes more than the Max MTU configured on any other Data-Plane Interface. When the Data plane interfaces are all at default 1500 MTU, Cluster Back Plane will be automatically set to 1578 (1500 + 78) MTU. If a Backplane interface is reset to Data Plane Interface, then the 1578 MTU will be automatically reset to the default MTU of 1500(or whatever lesser default value). If any data plane interface of a Cluster is configured with a Jumbo MTU (> 1500), then all backplane interfaces require to be configured with a minimum MTU of 'Highest Data Plane MTU in the Cluster + 78'. That makes the maximum Jumbo MTU for any Data-Plane Interface in a Cluster System to be '9138 (9216 - 78)., where 9216 is the maximum Jumbo MTU. On certain Virtualized / Cloud Platforms, the maximum possible MTU is restricted to a lesser value, Similar calculation can be applied, Maximum Data Plane MTU in Cluster = (Maximum possible MTU - 78). Default value: 1500 Minimum value: 1500 Maximum value: 9216

flowControl Required flow control for the LA channel.

Possible values: OFF, RX, TX, RXTX, ON Default value: OFF

haMonitor The state of HA monitoring for the LA channel.

Possible values: ON, OFF Default value: ON

haHeartbeat The state of HA HEARTBEAT SEND config for the LA channel.

Possible values: OFF, ON Default value: ON

tagall The appliance adds a four-byte 802.1q tag to every packet sent on this channel. ON applies tags for all the VLANs that are bound to this channel. OFF, applies the tag for all VLANs other than the native VLAN.

Possible values: ON, OFF Default value: OFF

ifAlias The alias name for the interface. Default value: " "

throughput Low threshold value for the throughput of the LA channel, in Mbps. In an high availability (HA) configuration, failover is triggered when the LA channel has HA MON enabled and the throughput is below the specified threshold. Minimum value: 0 Maximum value: 160000

lrMinThroughput Specifies the minimum throughput threshold (in Mbps) to be met by the active subchannel. Setting this parameter automatically divides an LACP channel into logical subchannels, with one subchannel active and the others in standby mode. When the maximum supported throughput of the active channel falls below the lrMinThroughput value, link failover occurs and a standby subchannel becomes active. Minimum value: 0 Maximum value: 80000

linkRedundancy Link Redundancy for Cluster LAG.

Possible values: ON, OFF Default value: OFF

bandwidthHigh High threshold value for the bandwidth usage of the LA channel, in Mbps. The Citrix ADC generates an SNMP trap message when the bandwidth usage of the LA channel is greater than or equal to the specified high threshold value. Minimum value: 0 Maximum value: 160000

bandwidthNormal Normal threshold value for the bandwidth usage of the LA channel, in Mbps. When the bandwidth usage of the LA channel returns to less than or equal to the specified normal threshold after exceeding the high threshold, the Citrix ADC generates an SNMP trap message to indicate that the bandwidth usage has returned to normal. Minimum value: 0 Maximum value: 160000

unset channel

Use this command to remove channel settings.Refer to the set channel command for meanings of the arguments.

Synopsis

unset channel <id>

ci

The following operations can be performed on "ci":

show ci

Displays all the critical interfaces of the Citrix ADC. In a High Availability configuration, an interface that has HA MON enabled and is not bound to any FIS, is a critical interface. Failure of any critical interface triggers HA failover.

Synopsis

show ci

Arguments

Output

ifaces Interfaces that are critical for the appliance to operate in high availability mode.

devno count stateflag

Example

```
show ci Critical Interfaces: LO/1 1/2
```

fis

The following operations can be performed on "fis":

rm| unbind| show| add| bind|

rm fis

Removes an FIS from the Citrix ADC. When an FIS is removed, its interfaces are marked as critical interfaces.

Synopsis

rm fis <name>

Arguments

name Name of the FIS that you want to remove from the Citrix ADC.

unbind fis

Unbinds the specified interfaces from a FIS. An unbound interface becomes a critical interface if it is enabled and HA MON is on.

Synopsis

unbind fis <name> <ifnum> ...

Arguments

name Name of the FIS from which to unbind interfaces.

ifnum Interfaces to unbind from the FIS, specified in slot/port notation (for example, 1/3). Use spaces to separate multiple entries.

show fis

Displays the configured FISs.

Synopsis

show fis

Arguments

name The name of the FIS configured on the appliance.

Output

ifaces Interfaces to be bound to the FIS, in slot/port notation (for example, 1/3).

stateflag Used internally for display.

ifnum Interface to be bound to the FIS, specified in slot/port notation (for example, 1/3)

ownerNode ID of the cluster node for which you are creating the FIS. Can be configured only through the cluster IP address.

devno count

Example

```
show fis
```

1. ```
   FIS: fis1

   Member Interfaces : 1/1
   ```

Done

add fis

Adds a failover interface set (FIS) to the Citrix ADC. A FIS is a logical group of interfaces. In an HA configuration, using a FIS is a way to prevent failover by grouping interfaces so that, when one interface fails, other functioning interfaces are still available. A FIS can also be configured for the nodes of a Citrix ADC cluster.

Synopsis

add fis <name>

Arguments

name Name for the FIS to be created. Leading character must be a number or letter. Other characters allowed, after the first character, are @ _ - . (period) : (colon) # and space ( ). Note: In a cluster setup, the FIS name on each node must be unique.

ownerNode ID of the cluster node for which you are creating the FIS. Can be configured only through the cluster IP address. Default value: -1 Minimum value: 0 Maximum value: 31

bind fis

Binds the specified interfaces to a FIS.

Synopsis

bind fis <name> <ifnum> ...

Arguments

name The name of the FIS to which you want to bind interfaces.

ifnum Interface to be bound to the FIS, specified in slot/port notation (for example, 1/3).

forwardingSession

The following operations can be performed on "forwardingSession":
   ```

set| show| rm| add|

set forwardingSession

Modifies parameters of a forwarding session rule.

Synopsis

set forwardingSession <name>

Arguments

name Name of the forwarding session rule. Required for identifying the forwarding session rule.

connfailover Synchronize connection information with the secondary appliance in a high availability (HA) pair. That is, synchronize all connection-related information for the forwarding session.

Possible values: ENABLED, DISABLED Default value: DISABLED

sourceroutecache Cache the source ip address and mac address of the DA servers.

Possible values: ENABLED, DISABLED Default value: DISABLED

processLocal Enabling this option on forwarding session will not steer the packet to flow processor. Instead, packet will be routed.

Possible values: ENABLED, DISABLED Default value: DISABLED

acl6name Name of any configured ACL6 whose action is ALLOW. The rule of the ACL6 is used as a forwarding session rule.

aclname Name of any configured ACL whose action is ALLOW. The rule of the ACL is used as a forwarding session rule.

Example

set forwardsession fw1 -connfailover enabled.

show forwardingSession

Displays the settings of all forwarding session rules configured on the Citrix ADC, or of the specified forwarding session rule.

Synopsis

show forwardingSession

Arguments

name Name of the forwarding session rule whose details you want to display.

Output

network An IPv4 network address or IPv6 prefix of a network from which the forwarded traffic originates or to which it is destined.

netmask Subnet mask associated with the network.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

aclname Name of any configured ACL whose action is ALLOW. The rule of the ACL is used as a forwarding session rule.

acl6name Name of any configured ACL6 whose action is ALLOW. The rule of the ACL6 is used as a forwarding session rule.

connfailover Synchronize connection information with the secondary appliance in a high availability (HA) pair. That is, synchronize all connection-related information for the forwarding session.

sourceroutecache Cache the source ip address and mac address of the DA servers.

processLocal Enabling this option on forwarding session will not steer the packet to flow processor. Instead, packet will be routed.

devno count stateflag

rm forwardingSession

Removes a forwarding session rule from the Citrix ADC.

Synopsis

rm forwardingSession <name>

Arguments

name Name of the forwarding session rule to be removed.

Example

rm forwardsession name.

add forwardingSession

Adds a forwarding session rule, which creates forwarding-session entries for traffic that originates from or is destined for a particular network and is forwarded by the Citrix ADC. By default, the appliance does not create session entries for traffic that only forwards (L3 mode). Add a forwarding session rule for a case in which a client request that the appliance forwards to a server results in a response that has to return by the same path

Synopsis

add forwardingSession <name> ((<network>) | -acl6name <string> | -aclname <string>)

Arguments

name Name for the forwarding session rule. Can begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the rule is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my rule" or 'my rule').

network An IPv4 network address or IPv6 prefix of a network from which the forwarded traffic originates or to which it is destined.

netmask Subnet mask associated with the network.

acl6name Name of any configured ACL6 whose action is ALLOW. The rule of the ACL6 is used as a forwarding session rule.

aclname Name of any configured ACL whose action is ALLOW. The rule of the ACL is used as a forwarding session rule.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

connfailover Synchronize connection information with the secondary appliance in a high availability (HA) pair. That is, synchronize all connection-related information for the forwarding session.

Possible values: ENABLED, DISABLED Default value: DISABLED

sourceroutecache Cache the source ip address and mac address of the DA servers.

Possible values: ENABLED, DISABLED Default value: DISABLED

processLocal Enabling this option on forwarding session will not steer the packet to flow processor. Instead, packet will be routed.

Possible values: ENABLED, DISABLED Default value: DISABLED

inat

The following operations can be performed on "inat":

add| rm| stat| unset| set| show|

add inat

Adds an INAT rule to the Citrix ADC. When a packet generated by a client matches the conditions specified in the INAT rule, the appliance translates the packet's public destination IP address to a private destination IP address and forwards the packet to the server at that address.

Synopsis

add inat <name>@ <publicIP>@ <privateIP>@

Arguments

name Name for the Inbound NAT (INAT) entry. Leading character must be a number or letter. Other characters allowed, after the first character, are @ _ - . (period) : (colon) # and space ( ).

publicIP Public IP address of packets received on the Citrix ADC. Can be aNetScaler-owned VIP or VIP6 address.

privateIP IP address of the server to which the packet is sent by the Citrix ADC. Can be an IPv4 or IPv6 address.

mode Stateless translation.

Possible values: STATELESS

tcpproxy Enable TCP proxy, which enables the Citrix ADC to optimize the RNAT TCP traffic by using Layer 4 features.

Possible values: ENABLED, DISABLED Default value: DISABLED

ftp Enable the FTP protocol on the server for transferring files between the client and the server.

Possible values: ENABLED, DISABLED Default value: DISABLED

tftp To enable/disable TFTP (Default DISABLED).

Possible values: ENABLED, DISABLED Default value: DISABLED

usip Enable the Citrix ADC to retain the source IP address of packets before sending the packets to the server.

Possible values: ON, OFF Default value: VAL_NOT_SET

usnip Enable the Citrix ADC to use a SNIP address as the source IP address of packets before sending the packets to the server.

Possible values: ON, OFF Default value: VAL_NOT_SET

proxyIP Unique IP address used as the source IP address in packets sent to the server. Must be a MIP or SNIP address.

useproxyport Enable the Citrix ADC to proxy the source port of packets before sending the packets to the server.

Possible values: ENABLED, DISABLED Default value: ENABLED

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

connfailover Synchronize connection information with the secondary appliance in a high availability (HA) pair. That is, synchronize all connection-related information for the INAT session

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

add nat mynat 1.2.3.4 192.168.1.100

rm inat

Remove the specified Inbound NAT configuration.

Synopsis

rm inat <name>@

Arguments

name Name of the Inbound NAT entry to be removed from the Citrix ADC.

Example

rm nat mynat.

stat inat

Display statistics for inat sessions.

Synopsis

stat inat

Arguments

name The INAT.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

TCP Packets translated (V4->V6) (nat46TotTcp46) Total TCP packets translated (V4->v6).

UDP Packets translated (V4->V6) (nat46TotUdp46) Total UDP packets translated (V4->v6).

ICMP Packets translated (V4->V6) (nat46TotIcmp46) Total ICMP packets translated (V4->v6).

Total IPV4 packets dropped (nat46Totdrop46) Total IPV4 packets dropped.

TCP Packets translated (V6->V4) (nat46TotTcp64) Total TCP packets translated (V6->v4).

UDP Packets translated (V6->V4) (nat46TotUdp64) Total UDP packets translated (V6->v4).

ICMP Packets translated (V6->V4) (nat46TotIcmp64) Total ICMP packets translated (V6->v4).

Total IPV6 packets dropped (nat46Totdrop64) Total IPV6 packets dropped.

TCP Packets translated (V4->V6) (inatNat46Tcp46) TCP packets translated (V4->v6).

UDP Packets translated (V4->V6) (inatNat46Udp46) UDP packets translated (V4->v6).

ICMP Packets translated (V4->V6) (inatNat46Icmp46) ICMP packets translated (V4->v6).

IPV4 packets dropped (inatNat46drop46) IPV4 packets dropped.

TCP Packets translated (V6->V4) (inatNat46Tcp64) TCP packets translated (V6->v4).

UDP Packets translated (V6->V4) (inatNat46Udp64) UDP packets translated (V6->v4).

ICMP Packets translated (V6->V4) (inatNat46Icmp64) ICMP packets translated (V6->v4).

IPV6 packets dropped (inatNat46drop64) IPV6 packets dropped.

Example

stat inat

Related Commands

- stat MapDomain

unset inat

Use this command to remove inat settings.Refer to the set inat command for meanings of the arguments.

Synopsis

unset inat <name>@

set inat

Modifies parameters of an INAT rule.

Synopsis

set inat <name>@

Arguments

name The name of the Inbound NAT (INAT) entry that you want to modify.

privateIP IP address of the server to which the packet is sent by the Citrix ADC. Can be an IPv4 or IPv6 address.

tcpproxy Enable TCP proxy, which enables the Citrix ADC to optimize the RNAT TCP traffic by using Layer 4 features.

Possible values: ENABLED, DISABLED Default value: DISABLED

ftp Enable the FTP protocol on the server for transferring files between the client and the server.

Possible values: ENABLED, DISABLED Default value: DISABLED

tftp To enable/disable TFTP (Default DISABLED).

Possible values: ENABLED, DISABLED Default value: DISABLED

usip Enable the Citrix ADC to retain the source IP address of packets before sending the packets to the server.

Possible values: ON, OFF Default value: VAL_NOT_SET

usnip Enable the Citrix ADC to use a SNIP address as the source IP address of packets before sending the packets to the server.

Possible values: ON, OFF Default value: VAL_NOT_SET

proxyIP A unique IP address used as the source IP address in packets sent to the server. Must be a MIP or SNIP address.

useproxyport Enable the Citrix ADC to proxy the source port of packets before sending the packets to the server.

Possible values: ENABLED, DISABLED Default value: ENABLED

connfailover Synchronize connection information with the secondary appliance in a high availability (HA) pair. That is, synchronize all connection-related information for the INAT session

Possible values: ENABLED, DISABLED Default value: DISABLED

mode Stateless translation.

Possible values: STATELESS

Example

set nat mynat -tcpproxy ENABLED

show inat

show all configured inbound NAT.

Synopsis

show inat

Arguments

name Name for the Inbound NAT (INAT) entry. Leading character must be a number or letter. Other characters allowed, after the first character, are @ _ - . (period) : (colon) # and space ( ).

Output

publicIP Public IP address of packets received on the Citrix ADC. Can be aNetScaler-owned VIP or VIP6 address.

privateIP IP address of the server to which the packet is sent by the Citrix ADC. Can be an IPv4 or IPv6 address.

proxyIP Source IP address for connection to a server.

tcpproxy Enable TCP proxy, which enables the Citrix ADC to optimize the RNAT TCP traffic by using Layer 4 features.

ftp Enable the FTP protocol on the server for transferring files between the client and the server.

tftp To enable/disable TFTP (Default DISABLED).

usip Enable the Citrix ADC to retain the source IP address of packets before sending the packets to the server.

usnip Enable the Citrix ADC to use a SNIP address as the source IP address of packets before sending the packets to the server.

useproxyport Enable the Citrix ADC to proxy the source port of packets before sending the packets to the server.

flags Flags for different modes

mode Stateless translation.

connfailover Synchronize connection information with the secondary appliance in a high availability (HA) pair. That is, synchronize all connection-related information for the INAT session

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

devno count stateflag

Example

show nat

inatparam

The following operations can be performed on "inatparam":

unset| set| show|

unset inatparam

Unset the inat parameter.Refer to the set inatparam command for meanings of the arguments.

Synopsis

unset inatparam [-nat46v6Prefix]

Example

unset inatparam -nat46v6Prefix -td 1

set inatparam

Set the inat parameter

Synopsis

set inatparam [-nat46v6Prefix <ipv6_addr|*>]

Arguments

nat46v6Prefix The prefix used for translating packets received from private IPv6 servers into IPv4 packets. This prefix has a length of 96 bits (128-32 = 96). The IPv6 servers embed the destination IP address of the IPv4 servers or hosts in the last 32 bits of the destination IP address field of the IPv6 packets. The first 96 bits of the destination IP address field are set as the IPv6 NAT prefix. IPv6 packets addressed to this prefix have to be routed to the Citrix ADC to ensure that the IPv6-IPv4 translation is done by the appliance.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Default value: 0 Minimum value: 0 Maximum value: 4094

nat46IgnoreTOS Ignore TOS.

Possible values: YES, NO Default value: NO

nat46ZeroCheckSum Calculate checksum for UDP packets with zero checksum

Possible values: ENABLED, DISABLED Default value: ENABLED

nat46v6Mtu MTU setting for the IPv6 side. If the incoming IPv4 packet greater than this, either fragment or send icmp need fragmentation error. Default value: 1280 Minimum value: 1280 Maximum value: 9216

nat46FragHeader When disabled, translator will not insert IPv6 fragmentation header for non fragmented IPv4 packets

Possible values: ENABLED, DISABLED Default value: ENABLED

Example

set inat parameter -nat46ignoretos YES

show inatparam

Show the inat parameters.

Synopsis

show inatparam

Arguments

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Default value: 0 Minimum value: 0 Maximum value: 4094

Output

nat46v6Prefix The prefix used for translating packets received from private IPv6 servers into IPv4 packets. This prefix has a length of 96 bits (128-32 = 96). The IPv6 servers embed the destination IP address of the IPv4 servers or hosts in the last 32 bits of the destination IP address field of the IPv6 packets. The first 96 bits of the destination IP address field are set as the IPv6 NAT prefix. IPv6 packets addressed to this prefix have to be routed to the Citrix ADC to ensure that the IPv6-IPv4 translation is done by the appliance.

nat46IgnoreTOS Ignore TOS.

nat46ZeroCheckSum Calculate checksum for UDP packets with zero checksum

nat46v6Mtu MTU setting for the IPv6 side. If the incoming IPv4 packet greater than this, either fragment or send icmp need fragmentation error.

nat46FragHeader When disabled, translator will not insert IPv6 fragmentation header for non fragmented IPv4 packets

setcmdflag devno count stateflag

Example

show inat params

inatsession

The following operations can be performed on "inatsession":

stat inatsession

Display statistics for stateful inat sessions.

Synopsis

stat inatsession

Arguments

name INAT name

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Total INAT Session hits (globalInatHits) Total INAT Session hits

Total INAT Current sessions (globalCurInatSessions) Total INAT current sessions

Total INAT Received Bytes (globalInatReceiveBytes) Total INAT Received Bytes

Total INAT Sent Bytes (globalInatSentBytes) Total INAT Sent Bytes

Total INAT Packets Received (globalInatPktReceived) Total INAT Packets Received

Total INAT Packets Sent (globalInatPktSent) Total INAT Packets Sent

INAT total sessions (inatTotHits) INAT total sessions

INAT Current sessions (inatCurSessions) INAT current sessions

INAT total Received Bytes (inatTotReceiveBytes) INAT total Received Bytes

INAT total Sent Bytes (inatTotSentBytes) INAT total Sent Bytes

INAT total Packets Received (inatTotpktreceived) INAT total Packets Received

INAT total Packets Sent (inatTotpktsent) INAT total Packets Sent

Example

stat inatsession

Related Commands

- stat MapDomain

interface

The following operations can be performed on "interface":

set| enable| unset| reset| show| clear| stat| disable|

set interface

Modifies the parameters of an interface.

Synopsis

set interface <id>@ [-trunkAllowedVlan <int> ...] [-bandwidthHigh <positive_integer>]

Arguments

id ID of the Interface whose parameters you want to modify. For a Citrix ADC, specify the interface in C/U notation (for example, 1/3). For a cluster configuration, specify the interface in N/C/U notation (for example, 2/1/3). where C can take one of the following values:

- 0 - Indicates a management interface.
- 1 - Indicates a 1 Gbps port.
- 10 - Indicates a 10 Gbps port. U is a unique integer for representing an interface in a particular port group. N is the ID of the node to which an interface belongs in a cluster configuration. Use spaces to separate multiple entries.

speed Ethernet speed of the interface, in Mbps. Notes:

- If you set the speed as AUTO, the Citrix ADC attempts to auto-negotiate or auto-sense the link speed of the interface when it is UP. You must enable auto negotiation on the interface.

- If you set a speed other than AUTO, you must specify the same speed for the peer network device. Mismatched speed and duplex settings between the peer devices of a link lead to link errors, packet loss, and other errors. Some interfaces do not support certain speeds. If you specify an unsupported speed, an error message appears.

Possible values: AUTO, 10, 100, 1000, 10000, 25000, 40000, 50000, 100000 Default value: AUTO

duplex The duplex mode for the interface. Notes:* If you set the duplex mode to AUTO, the Citrix ADC attempts to auto-negotiate the duplex mode of the interface when it is UP. You must enable auto negotiation on the interface. If you set a duplex mode other than AUTO, you must specify the same duplex mode for the peer network device. Mismatched speed and duplex settings between the peer devices of a link lead to link errors, packet loss, and other errors.

Possible values: AUTO, HALF, FULL Default value: AUTO

flowControl 802.3x flow control setting for the interface. The 802.3x specification does not define flow control for 10 Mbps and 100 Mbps speeds, but if a Gigabit Ethernet interface operates at those speeds, the flow control settings can be applied. The flow control setting that is finally applied to an interface depends on auto-negotiation. With the ON option, the peer negotiates the flow control, but the appliance then forces two-way flow control for the interface.

Possible values: OFF, RX, TX, RXTX, ON Default value: OFF

autoneg Auto-negotiation state of the interface. With the ENABLED setting, the Citrix ADC auto-negotiates the speed and duplex settings with the peer network device on the link. The Citrix ADC appliance auto-negotiates the settings of only those parameters (speed or duplex mode) for which the value is set as AUTO.

Possible values: DISABLED, ENABLED Default value: NSA_DVC_AUTONEG_ON

haMonitor In a High Availability (HA) configuration, monitor the interface for failure events. In an HA configuration, an interface that has HA MON enabled and is not bound to any Failover Interface Set (FIS), is a critical interface. Failure or disabling of any critical interface triggers HA failover.

Possible values: ON, OFF Default value: ON

haHeartbeat In a High Availability (HA) or Cluster configuration, configure the interface for sending heartbeats. In an HA or Cluster configuration, an interface that has HA Heartbeat disabled should not send the heartbeats.

Possible values: OFF, ON Default value: ON

mtu The Maximum Transmission Unit (MTU) is the largest packet size, measured in bytes excluding 14 bytes ethernet header and 4 bytes CRC, that can be transmitted and received by an interface. The default value of MTU is 1500 on all the interface of Citrix ADC, some Cloud Platforms will restrict Citrix ADC to use the lesser default value. Any MTU value more than 1500 is called Jumbo MTU and will make the interface as jumbo enabled. The Maximum Jumbo MTU in Citrix ADC is 9216, however, some Virtualized / Cloud Platforms will have lesser Maximum Jumbo MTU Value (9000). In the case of Cluster, the Backplane interface requires an MTU value of 78 bytes more than the Max MTU configured on any other Data-Plane Interface. When the Data plane interfaces are all at default 1500 MTU, Cluster Back Plane will be automatically set to 1578 (1500 + 78) MTU. If a Backplane interface is reset to Data Plane Interface, then the 1578 MTU will be automatically reset to the default MTU of 1500(or whatever lesser default value). If any data plane interface of a Cluster is configured with a Jumbo MTU (> 1500), then all backplane interfaces require to be configured with a minimum MTU of 'Highest Data Plane MTU in the Cluster + 78'. That makes the maximum Jumbo MTU for any Data-Plane Interface in a Cluster System to be '9138 (9216 - 78)., where 9216 is the maximum Jumbo MTU. On certain Virtualized / Cloud Platforms, the maximum possible MTU is restricted to a lesser value, Similar calculation can be applied, Maximum Data Plane MTU in Cluster = (Maximum possible MTU - 78). Default value: 1500 Minimum value: 1500 Maximum value: 9216

ringsize The receive ringsize of the interface. A higher number provides more number of buffers in handling incoming traffic. Default value: 2048 Minimum value: 512 Maximum value: 16384

ringtype The receive ringtype of the interface (Fixed or Elastic). A fixed ring type pre-allocates configured number of buffers irrespective of traffic rate. In contrast, an elastic ring, expands and shrinks based on incoming traffic rate.

Possible values: Elastic, Fixed Default value: Elastic

tagall Add a four-byte 802.1q tag to every packet sent on this interface. The ON setting applies the tag for this interface's native VLAN. OFF applies the tag for all VLANs other than the native VLAN.

Possible values: ON, OFF Default value: OFF

trunkmode Accept and send 802.1q VLAN tagged packets, based on Allowed Vlan List of this interface.

Possible values: ON, OFF Default value: OFF

trunkAllowedVlan VLAN ID or range of VLAN IDs will be allowed on this trunk interface. In the command line interface, separate the range with a hyphen. For example: 40-90. Minimum value: 1 Maximum value: 4094

lacpMode Bind the interface to a LA channel created by the Link Aggregation control protocol (LACP). Available settings function as follows:

- Active - The LA channel port of the Citrix ADC generates LACPDU messages on a regular basis, regardless of any need expressed by its peer device to receive them.
- Passive - The LA channel port of the Citrix ADC does not transmit LACPDU messages unless the peer device port is in the active mode. That is, the port does not speak unless spoken to.
- Disabled - Unbinds the interface from the LA channel. If this is the only interface in the LA channel, the LA channel is removed.

Possible values: DISABLED, ACTIVE, PASSIVE Default value: DISABLED

lacpKey Integer identifying the LACP LA channel to which the interface is to be bound. For an LA channel of the Citrix ADC, this digit specifies the variable x of an LA channel in LA/x notation, where x can range from 1 to 8. For example, if you specify 3 as the LACP key for an LA channel, the interface is bound to the LA channel LA/3. For an LA channel of a cluster configuration, this digit specifies the variable y of a cluster LA channel in CLA/(y-4) notation, where y can range from 5 to 8. For example, if you specify 6 as the LACP key for a cluster LA channel, the interface is bound to the cluster LA channel CLA/2. Minimum value: 1 Maximum value: 8

lagtype Type of entity (Citrix ADC or cluster configuration) for which to create the channel.

Possible values: NODE, CLUSTER Default value: NODE

lacpPriority LACP port priority, expressed as an integer. The lower the number, the higher the priority. The Citrix ADC limits the number of interfaces in an LA channel to sixteen. Default value: 32768 Minimum value: 1 Maximum value: 65535

lacpTimeout Interval at which the Citrix ADC sends LACPDU messages to the peer device on the LA channel. Available settings function as follows: LONG - 30 seconds. SHORT - 1 second.

Possible values: LONG, SHORT Default value: NSA_LACP_TIMEOUT_LONG

ifAlias Alias name for the interface. Used only to enhance readability. To perform any operations, you have to specify the interface ID. Default value: " "

throughput Low threshold value for the throughput of the interface, in Mbps. In an HA configuration, failover is triggered if the interface has HA MON enabled and the throughput is below the specified the threshold. Minimum value: 0 Maximum value: 160000

linkRedundancy Link Redundancy for Cluster LAG.

Possible values: ON, OFF Default value: OFF

bandwidthHigh High threshold value for the bandwidth usage of the interface, in Mbps. The Citrix ADC generates an SNMP trap message when the bandwidth usage of the interface is greater than or equal to the specified high threshold value. Minimum value: 0 Maximum value: 160000

bandwidthNormal Normal threshold value for the bandwidth usage of the interface, in Mbps. When the bandwidth usage of the interface becomes less than or equal to the specified normal threshold after exceeding the high threshold, the Citrix ADC generates an SNMP trap message to indicate that the bandwidth usage has returned to normal. Minimum value: 0 Maximum value: 160000

lldpmode Link Layer Discovery Protocol (LLDP) mode for an interface. The resultant LLDP mode of an interface depends on the LLDP mode configured at the global and the interface levels.

Possible values: NONE, TRANSMITTER, RECEIVER, TRANSCEIVER

lrsetPriority LRSET port priority, expressed as an integer ranging from 1 to 1024. The highest priority is 1. The Citrix ADC limits the number of interfaces in an LRSET to 8. Within a LRSET the highest LR Priority Interface is considered as the first candidate for the Active interface, if the interface is UP. Default value: 1024 Minimum value: 1 Maximum value: 1024

enable interface

Enables the interface. If the link is active, it can transmit and receive packets. Note: To view the status of an interface, use the show interface command.

Synopsis

enable interface <id>@

Arguments

id Interface number, in C/U format, where C can take one of the following values:

- 0 - Indicates a management interface.
- 1 - Indicates a 1 Gbps port.
- 10 - Indicates a 10 Gbps port.
- LA - Indicates a link aggregation port.
- LO - Indicates a loop back port. U is a unique integer for representing an interface in a particular port group.

unset interface

Use this command to remove interface settings.Refer to the set interface command for meanings of the arguments.

Synopsis

unset interface <id>@

reset interface

Restarts the interface but leaves the administrative state ENABLED or DISABLED and configuration unchanged. The link pertaining to the interface is reestablished with the existing settings.

Synopsis

reset interface <id>@

Arguments

id Interface number, in C/U format, where C can take one of the following values:

- 0 - Indicates a management interface.
- 1 - Indicates a 1 Gbps port.
- 10 - Indicates a 10 Gbps port.
- LA - Indicates a link aggregation port.
- LO - Indicates a loop back port. U is a unique integer for representing an interface in a particular port group.

show interface

Displays the settings of all interfaces or of the specified interface on the Citrix ADC. To display the settings of all interfaces, run the command without any parameters. To display the settings of a particular interface, specify the ID of the interface.

Synopsis

show interface show interface stats - alias for 'stat interface'

Arguments

id Interface number, in C/U format, where C can take one of the following values:

- 0 - Indicates a management interface.
- 1 - Indicates a 1 Gbps port.
- 10 - Indicates a 10 Gbps port.
- LA - Indicates a link aggregation port.
- LO - Indicates a loop back port. U is a unique integer for representing an interface in a particular port group.

Output

stateflag deviceName Name of the interface.

unit Unit number for this interface, signifying the sequence number in which this interface is discovered on this Citrix ADC.

description Display the type of interface, the speeds at which this interface can operate, and, if applicable, the type of SFP,.

flags Flags for this interface. Used for communicating the device states.

mtu The Maximum Transmission Unit (MTU) is the largest packet size, measured in bytes excluding 14 bytes ethernet header and 4 bytes CRC, that can be transmitted and received by an interface. The default value of MTU is 1500 on all the interface of Citrix ADC, some Cloud Platforms will restrict Citrix ADC to use the lesser default value. Any MTU value more than 1500 is called Jumbo MTU and will make the interface as jumbo enabled. The Maximum Jumbo MTU in Citrix ADC is 9216, however, some Virtualized / Cloud Platforms will have lesser Maximum Jumbo MTU Value (9000). In the case of Cluster, the Backplane interface requires an MTU value of 78 bytes more than the Max MTU configured on any other Data-Plane Interface. When the Data plane interfaces are all at default 1500 MTU, Cluster Back Plane will be automatically set to 1578 (1500 + 78) MTU. If a Backplane interface is reset to Data Plane Interface, then the 1578 MTU will be automatically reset to the default MTU of 1500(or whatever lesser default value). If any data plane interface of a Cluster is configured with a Jumbo MTU (> 1500), then all backplane interfaces require to be configured with a minimum MTU of 'Highest Data Plane MTU in the Cluster + 78'. That makes the maximum Jumbo MTU for any Data-Plane Interface in a Cluster System to be '9138 (9216 - 78)., where 9216 is the maximum Jumbo MTU. On certain Virtualized / Cloud Platforms, the maximum possible MTU is restricted to a lesser value, Similar calculation can be applied, Maximum Data Plane MTU in Cluster = (Maximum possible MTU - 78).

actualMtu MTU for this interface (the largest frame that can transit this interface).

vlan Native VLAN for this interface.

mac MAC address for this interface.

uptime Duration for which the interface has been UP (Example: 3 hours 1 minute 1 second). This value is reset when the interface state changes to DOWN..

downTime Duration for which the interface has been DOWN. This value is reset when the interface state changes to UP.(Example: 3 hours 1 minute 1 second).

ringsize The receive ringsize of the interface. A higher number provides more number of buffers in handling incoming traffic.

ringtype The receive ringtype of the interface (Fixed or Elastic). A fixed ring type pre-allocates configured number of buffers irrespective of traffic rate. In contrast, an elastic ring, expands and shrinks based on incoming traffic rate.

actualringsize Actual receive ringsize of the interface. This will be same as configured receive ringsize when ringtype is Fixed whereas it denotes the current number of receive buffers allocated when ringtype is Elastic

reqMedia Requested media setting for this interface.

reqSpeed Requested speed setting for this interface.

reqDuplex Requested duplex setting for this interface.

reqFlowcontrol Requested flow control setting for this interface.

media speed Ethernet speed of the interface, in Mbps. Notes:

- If you set the speed as AUTO, the Citrix ADC attempts to auto-negotiate or auto-sense the link speed of the interface when it is UP. You must enable auto negotiation on the interface.
- If you set a speed other than AUTO, you must specify the same speed for the peer network device. Mismatched speed and duplex settings between the peer devices of a link lead to link errors, packet loss, and other errors. Some interfaces do not support certain speeds. If you specify an unsupported speed, an error message appears.

duplex The duplex mode for the interface. Notes:* If you set the duplex mode to AUTO, the Citrix ADC attempts to auto-negotiate the duplex mode of the interface when it is UP. You must enable auto negotiation on the interface. If you set a duplex mode other than AUTO, you must specify the same duplex mode for the peer network device. Mismatched speed and duplex settings between the peer devices of a link lead to link errors, packet loss, and other errors.

flowControl 802.3x flow control setting for the interface. The 802.3x specification does not define flow control for 10 Mbps and 100 Mbps speeds, but if a Gigabit Ethernet interface operates at those speeds, the flow control settings can be applied. The flow control setting that is finally applied to an interface depends on auto-negotiation. With the ON option, the peer negotiates the flow control, but the appliance then forces two-way flow control for the interface.

media Actual media setting for this interface.

speed Actual speed setting for this interface.

duplex Actual duplex setting for this interface.

flowControl Actual flow control setting for this interface.

Mode Interface Link Aggregation mode (Auto/Manual) setting.

Mode The mode(AUTO/MANNUAL) for the LA channel.

haMonitor HA monitor enabled or disabled for this interface.

haHeartbeat HA Hearbeat send enabled or disabled for this interface.

state Link state of the interface (UP/DOWN).

autoneg Interface autonegotiation enabled or disabled.

autonegResult Actual auto-negotiation setting for this interface.

tagged VLAN tags setting on this channel.

tagall VLAN tagging behavior on this interface. With the ON setting,, packets are tagged with all the VLANs that are bound to this interface. With the OFF setting, packets are tagged with the native VLAN.

trunk This argument is deprecated by tagall.

trunkmode Accept and send 802.1q VLAN tagged packets, based on Allowed Vlan List of this interface.

trunkAllowedVlan VLAN ID or range of VLAN IDs will be allowed on this trunk interface. In the command line interface, separate the range with a hyphen. For example: 40-90.

taggedAny Interface setting to accept/drop all tagged packets.

taggedAutolearn Dynamic VLAN membership autolearning enabled or disabled on this interface.

hangDetect Hang detection enabled or disabled for this interface.

hangReset Hang reset enabled or disabled for this interface.

linkState The current state of the link associated with the interface. For logical interfaces (LA), the state of the link is dependent on the state of the slave interfaces. For the link to be UP at least one of the slave interfaces needs to be UP.

intfState Current state of the specified interface. The interface state set to UP only if the link state is UP and administrative state is ENABLED.

rxpackets Number of packets received by an interface since the Citrix ADC was started or the interface statistics were cleared.

rxbytes Number of bytes received by an interface since the Citrix ADC was started or the interface statistics were cleared.

rxerrors Number of inbound packets dropped by the hardware on a specified interface since the Citrix ADC was started or the interface statistics were cleared. Packets can be dropped because of CRC, length (undersize or oversize), or alignment errors.

rxdrops Number of inbound packets dropped by the specified interface. Commonly dropped packets are multicast frames, spanning tree BPDUs, packets destined to a MAC not owned by the Citrix ADC when L2 mode is disabled, or packets tagged for a VLAN that is not bound to the interface. In most healthy networks, this statistic increments at a steady rate regardless of traffic load. A sharp spike in dropped packets generally indicates an issue with connected L2 switches, such as a forwarding database overflow resulting in packets being broadcast on all ports.

txpackets Number of packets transmitted by an interface since the Citrix ADC was started or the interface statistics were cleared.

txbytes Number of bytes transmitted by an interface since the Citrix ADC was started or the interface statistics were cleared.

txerrors Number of outbound packets dropped by the hardware on a specified interface since the Citrix ADC was started or the interface statistics were cleared. Packets can be dropped because of length (undersize or oversize) errors or a lack of resources. This statistic is available only for: (1) Loop back interface (LO) of all platforms. (2) All data ports on the Citrix ADC 12000 platform. (3) Management ports on the Citrix ADC MPX 15000 and 17000 platforms.

txdrops Number of packets dropped in transmission by the specified interface for one of the following reasons. (1) VLAN mismatch. (2) Oversized packets. (3) Interface congestion. (4) Loopback packets sent on non loop back interface.

inDisc Number of error-free inbound packets discarded by the specified interface because of a lack of resources (for example, insufficient receive buffers).

outDisc Number of error-free outbound packets discarded by the specified interface because of a lack of resources. This statistic is not available on: (1) 10G ports of Citrix ADC MPX 12500/12500/15500-10G platforms. (2) 10G data ports on Citrix ADC MPX 17500/19500/21500 platforms.

fctls Number of times flow control is performed on the specified interface because of received pause frames.

hangs Number of times the specified interface detected hangs in the transmit and receive paths since the Citrix ADC was started or the interface statistics were cleared.

stsStalls Number of times the status updates for a specified interface were stalled since the Citrix ADC was started or the interface statistics were cleared. A status stall is detected when the status of the interface is not updated by the NIC hardware within 0.8 seconds of the last update.

txStalls Number of times the interface stalled, when transmitting packets, since the Citrix ADC was started or the interface statistics were cleared. Transmit (Tx) stalls are detected when a packet posted for transmission is not transmitted in 4 seconds.

rxStalls Number of times the interface stalled, when receiving packets, since the Citrix ADC was started or the interface statistics were cleared. Receive (Rx) stalls are detected when the following conditions are met: (1)The link is up for more than 10 minutes. (2)Packets are transmitted, but no packets are received for 16 seconds.

bdgMacMoved Number of MAC moves between ports. A high rate of MAC moves typically indicates a bridge loop between two interfaces.

bdgMuted Number of times the specified interface stopped transmitting and receiving packets because of MAC moves between ports.

vmac Virtual MAC of this interface.

vmac6 Virtual MAC for IPv6 of this interface.

lacpMode The LACP mode of the specified interface. The possible values are:

1. Active: A port in active mode generates LACP protocol messages on a regular basis, regardless of any need expressed by its partner to receive them.
2. Passive: A port in passive mode is generally not transmit LACP messages unless its partner is in the active mode; that is, it does not communicate to the other appliance unless other appliance communicates with this appliance.

lacpKey Identifies the channel to which the interface is bound. The possible values are 1, 2, 3, and 4.

lacpPriority LACP port priority, expressed as an integer. The lower the number, the higher the priority. The Citrix ADC limits the number of interfaces in an LA channel to sixteen.

lacpTimeout Time to wait for the LACPDU. If an LACPDU is not received within this interval, the Citrix ADC markes the link partner port as DOWN. Possible values; Long, Short. Long lacptimeout is 90 sec and Short LACP timeout is 3 sec.

lagtype Type of entity (Citrix ADC or cluster configuration) for which to create the channel.

ifAlias Alias name for the interface. Used only to enhance readability. To perform any operations, you have to specify the interface ID.

reqThroughput Minimum required throughput for an interface. Failover is triggered if the operating throughput of a Link Aggregation (LA) channel for which HAMON is ON falls below this value. The possible values are:

1. 1000Mbps for 1G interfaces.
2. 10000Mbps for 10G interfaces.
3. 160000Mbps for Link Aggregation channels.

throughput Minimum required throughput for the interface.

linkRedundancy Link Redundancy for Cluster LAG.

throughput Actual throughput for the interface.

bandwidthHigh High threshold value for the bandwidth usage of the interface, in Mbps. The Citrix ADC generates an SNMP trap message when the bandwidth usage of the interface is greater than or equal to the specified high threshold value.

bandwidthNormal Normal threshold value for the bandwidth usage of the interface, in Mbps. When the bandwidth usage of the interface becomes less than or equal to the specified normal

threshold after exceeding the high threshold, the Citrix ADC generates an SNMP trap message to indicate that the bandwidth usage has returned to normal.

backplane The cluster backplane status of the interface. If the status is enabled, the interface is part of the cluster backplane. By default, the backplane status is disabled.

ifnum Contains the LA Master, if the interface is part of LA channel.

clearTime Time since the interface stats are cleared last time.

slavestate State of the member interfaces.

slavemedia Media type of the member interfaces.

slavespeed Speed of the member interfaces.

slaveduplex Duplex of the member interfaces.

slaveflowctl Flowcontrol of the member interfaces.

slavetime UP time of the member interfaces.

intftype Interface Type, this field will have the interface type either it is virtual, physical or loopback.

svmCmd New attribute added to identify the source of cmd, when SVM fires the nitro cmd, it will set the value of SVMCMD to be 1.

lacpActorMode

- Active - The LA channel port of the Citrix ADC generates LACPDU messages on a regular basis, regardless of any need expressed by its peer device to receive them.
- Passive - The LA channel port of the Citrix ADC does not transmit LACPDU messages unless the peer device port is in the active mode. That is, the port does not speak unless spoken to.
- Disabled - Unbinds the interface from the LA channel. If this is the only interface in the LA channel, the LA channel is removed.

lacpActorTimeout Interval at which the Citrix ADC sends LACPDU messages to the peer device on the LA channel. Available settings function as follows: LONG - 30 seconds. SHORT - 1 second.

lacpActorPriority LACP Actor Priority. A LACP port priority is configured on each port using LACP. LACP uses the port priority with the port number to form the port identifier. The port priority

determines which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

lacpActorPortno LACP Actor port number. LACP uses the port priority with the port number to form the port identifier.

lacpPartnerState LACP Partner State. Whether the port is in Active or Passive negotiating state.

lacpPartnerTimeout The timeout value for the information revieved in LACPDUs. It can have values as SHORT or LONG. The SHORT timeout is 3s and the LONG timeout is 90s.

lacpPartnerAggregation The Aggregation flag indicates that the participant will allow the link to be used as part of an aggregate. Otherwise the link is to be used as an individual link, i.e. not aggregated with any other.

lacpPartnerInsync The Synchronization flag indicates that the transmitting participant.s mux component is in sync with the system id and key information transmitted.

lacpPartnerCollecting The Collecting flag indicates that the participant.s collector, i.e. the reception component of the mux, is definitely on. If set the flag communicates collecting.

lacpPartnerDistributing The Distributing flag indicates that the participant.s distributor is not definitely off. If reset the flag indicates not distributing.

lacpPartnerDefaulted If the timer expires in the Expired state, the Receive Machine enters the Defaulted state.

lacpPartnerExpired If the LACPDUs are received for timeout period, the Receive Machine enters the Expired state and the timer is restarted with the timeout value of SHORT timeout

lacpPartnerPriority LACP Partner Priority. A LACP port priority is configured on each port using LACP. LACP uses the port priority with the port number to form the port identifier. The port priority determines which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

lacpPartnerSystemMac LACP Partner System MAC.

lacpPartnerSystemPriority LACP Partner System Priority. The LACP partner's system priority. The values for the priority range from 0 to 65535. The lower the value, the higher the system priority. The switch with the lower system priority value determines which links between LACP partner are active and which are in the standby for each LACP Channel.

lacpPartnerPortno LACP Partner Port number. LACP uses the port priority with the port number to form the port identifier.

lacpPartnerKey LACP Partner Key. The LACP key used by the partner port.

lacpActorAggregation The Aggregation flag indicates that the participant will allow the link to be used as part of an aggregate. Otherwise the link is to be used as an individual link, i.e. not aggregated with any other.

lacpActorInsync The Synchronization flag indicates that the transmitting participant.s mux component is in sync with the system id and key information transmitted.

lacpActorCollecting The Collecting flag indicates that the participant.s collector, i.e. the reception component of the mux, is definitely on. If set the flag communicates collecting.

lacpActorDistributing The Distributing flag indicates that the participant.s distributor is not definitely off. If reset the flag indicates not distributing.

lacpPortMuxState LACP Port MUX state. The state of the MUX control machine. The Mux Control Machine attaches the physical port to an aggregate port, using the Selection Logic to choose an appropriate port, and turns the distributor and collector for the physical port on or off as required by protocolinformation.

lacpPortRxStat LACP Port RX state. The state of the Receive machine. The Receive Machine maintains partner information, recording protocol information from LACPDUs sent by remote partner(s). Received information is subject to a timeout, and if sufficient time elapses the receive machine will revert to using default partner information.

lacpPortSelectState LACP Port SELECT state. The state of the SELECT state machine, It could be SELECTED or UNSELECTED.

lldpmode Link Layer Discovery Protocol (LLDP) mode for an interface. The resultant LLDP mode of an interface depends on the LLDP mode configured at the global and the interface levels.

lrsetPriority LRSET port priority, expressed as an integer ranging from 1 to 1024. The highest priority is 1. The Citrix ADC limits the number of interfaces in an LRSET to 8. Within a LRSET the highest LR Priority Interface is considered as the first candidate for the Active interface, if the interface is UP.

lrActiveIntf LR set member interface state(active/inactive).

devno count

Example

The output for the show interface command is as follows:

1.
```
Interface 0/1 (Gig Ethernet 10/100/1000 MBits) #4

flags=0x4021 &lt;ENABLED, UP, UP, autoneg, HAMON, 802.1q>

MTU=1500, native vlan=1, MAC=00:30:48:67:9a:9a, uptime 1039h54m28s

Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,

         throughput 0
```

2.
```
Interface 1/1 (Gig Ethernet, copper SFP) #3

flags=0x4021 &lt;ENABLED, UP, UP, autoneg, HAMON, BACKPLANE, 802.1q>

MTU=1500, native vlan=1, MAC=00:e0:ed:12:e8:b7, uptime 1039h54m28s

Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,

         throughput 0
```

3.
```
Interface 1/2 (Gig Ethernet, copper SFP) #2

flags=0x4001 &lt;ENABLED, DOWN, down, autoneg, HAMON, 802.1q>

MTU=1500, native vlan=1, MAC=00:e0:ed:12:e8:b6, downtime 1039h54m28s

Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,

         throughput 0
```

4.
```
Interface 1/3 (Gig Ethernet, copper SFP) #1

flags=0x4001 &lt;disabled, DOWN, down, autoneg, HAMON, 802.1q>

MTU=1500, native vlan=1, MAC=00:e0:ed:12:e8:b5, downtime 1039h54m33s

Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,
```

```
         throughput 0
```

5.
```
Interface 1/4 (Gig Ethernet, copper SFP) #0

flags=0x4001 &lt;disabled, UP, down, autoneg, HAMON, 802.1q>

MTU=1500, native vlan=1, MAC=00:e0:ed:12:e8:b4, downtime 1039h54m28s

Requested: media AUTO, speed AUTO, duplex AUTO, fctl OFF,

         throughput 0
```

Done

The output for the show interface 0/1 command is as follows:

```
 Interface 0/1 (Gig Ethernet 10/100/1000 MBits) #4

 flags=0xc020 &lt;ENABLED, UP, UP, autoneg, HAMON, 802.1q>

 MTU=1500, native vlan=1, MAC=00:30:48:67:9a:9a, uptime 0h00m40s

 Requested: media AUTO, speed AUTO, duplex AUTO, fctl RXTX,

          throughput 0

 Actual: media UTP, speed 1000, duplex FULL, fctl RXTX, throughput 1000



 RX: Pkts(27) Bytes(2034) Errs(0) Drops(27) Stalls(0)

 TX: Pkts(3) Bytes(170) Errs(0) Drops(22) Stalls(0)

 NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)

 Bandwidth thresholds are not set.
```

Done

clear interface

Resets the statistical counters of the specified interface.

Synopsis

clear interface <id>@

Arguments

id Interface number, in C/U format, where C can take one of the following values:

- 0 - Indicates a management interface.
- 1 - Indicates a 1 Gbps port.
- 10 - Indicates a 10 Gbps port.
- LA - Indicates a link aggregation port.
- LO - Indicates a loop back port. U is a unique integer for representing an interface in a particular port group.

stat interface

Displays the statistics of all interfaces or of the specified interface on the Citrix ADC. To display the statistics of all interfaces, run the command without any parameters. To display the statistics of a particular interface, specify the ID of the interface.

Synopsis

stat interface

Arguments

id Interface number, in C/U format, where C can take one of the following values:

- 0 - Indicates a management interface.
- 1 - Indicates a 1 Gbps port.
- 10 - Indicates a 10 Gbps port.
- LA - Indicates a link aggregation port.
- LO - Indicates a loop back port. U is a unique integer for representing an interface in a particular port group.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Interface State (IntfState) Current state of the specified interface. The interface state set to UP only if the link state is UP and administrative state is ENABLED .

Link uptime (UpTime) Duration for which the link is UP. This statistic is reset when the state changes to DOWN.

Link downtime (DnTime) Duration for which the link is DOWN. This statistic is reset when the state changes to UP.

Bytes received (Rx Bytes) Number of bytes received by an interface since the Citrix ADC was started or the interface statistics were cleared.

Bytes transmitted (Tx Bytes) Number of bytes transmitted by an interface since the Citrix ADC was started or the interface statistics were cleared.

Packets received (Rx Pkts) Number of packets received by an interface since the Citrix ADC was started or the interface statistics were cleared.

Packets transmitted (Tx Pkts) Number of packets transmitted by an interface since the Citrix ADC was started or the interface statistics were cleared.

Jumbo Packets Received (JumboRcv) Number of Jumbo Packets received on this interface.

Jumbo Packets Transmitted (JumboXmit) Number of Jumbo packets transmitted on this interface by upper layer, with TSO enabled actual trasmission size could be non Jumbo.

Tagged Packets Received on Trunk interface through allowed vlan list (TrunkRcv) Number of Tagged Packets received on this Trunk interface through Allowed VLan List.

Tagged Packets transmitted on Trunk interface through allowed vlan list (TrunkXmit) Number of Tagged Packets transmitted on this Trunk interface through Allowed VLan List.

Multicast packets (McastPkt) Number of multicast packets received by the specified interface since the Citrix ADC was started or the interface statistics were cleared.

NetScaler packets (NSPkt) Number of packets, destined to the Citrix ADC, received by an interface since the Citrix ADC was started or the interface statistics were cleared. The packets destined to Citrix ADC are those that have the same MAC address as that of an interface or a VMAC address owned by the Citrix ADC.

LACPDUs received (RxLacpdu) Number of Link Aggregation Control Protocol Data Units(LACPDUs) received by the specified interface since the Citrix ADC was started or the interface statistics were cleared.

LACPDUs transmitted (TxLacpdu) Number of Link Aggregation Control Protocol Data Units(LACPDUs) transmitted by the specified interface since the Citrix ADC was started or the interface statistics were cleared.

Error packets received (hw) (ErrRx) Number of inbound packets dropped by the hardware on a specified interface once the Citrix ADC starts or the interface statistics are cleared. This happens due to following reasons: 1)The hardware receives packets at a rate higher rate than that at which the software is processing packets. In this case, the hardware FIFO overruns and starts dropping the packets . 2)The specified interface fails to receive inbound packets from the appliance because of insufficient memory. 3)The specified interface receives packets with CRC errors (Alignment or Frame Check Sequence). 4)The specified interface receives overly long packets. 5)The specified interface receives packets with alignment errors. 6)The software does less buffering because it is running out of available memory. When hardware detects that there is no space into which to push newly arrived packets, it starts dropping them. 7)The specified interface receives packets with Frame Check Sequence (FCS) errors. 8)The specified interface receives packets smaller than 64 bytes. 9)The specified interface discards error-free inbound packets because of insufficient resources. For example: NIC buffers. 10)Packets are missed because of collision detection, link lost, physical decoding error, or MAC abort.

Error packets transmitted (hw) (ErrTx) Number of outbound packets dropped by the hardware on a specified interface since the Citrix ADC was started or the interface statistics were cleared. This could happen due to length (undersize or oversize) errors and lack of resources. This statistic

is available only for: (1) Loop back interface (LO) of all platforms. (2) All data ports on the Citrix ADC 12000 platform. (3) Management ports on the MPX 15000 and 17000 platforms.

Inbound packets discarded(hw) (InDisc) Number of error-free inbound packets discarded by the specified interface due to a lack of resources, for example, insufficient receive buffers.

Outbound packets discarded(hw) (OutDisc) Number of error-free outbound packets discarded by the specified interface due to a lack of resources. This statistic is not available on: (1) 10G ports of Citrix ADC MPX 12500/12500/15500-10G platforms. (2) 10G data ports on Citrix ADC MPX 17500/19500/21500 platforms.

Packets dropped in Rx (sw) (DrpRxPkt) Number of inbound packets dropped by the specified interface. Commonly dropped packets are multicast frames, spanning tree BPDUs, packets destined to a MAC not owned by the Citrix ADC when L2 mode is disabled, or packets tagged for a VLAN that is not bound to the interface. This statistic will increment in most healthy networks at a steady rate regardless of traffic load. If a sharp spike in dropped packets occurs, it generally indicates an issue with connected L2 switches, such as a forwarding database overflow resulting in packets being broadcast on all ports.

Packets dropped in Tx (sw) (DrpTxPkt) Number of packets dropped in transmission by the specified interface due to one of the following reasons. (1) VLAN mismatch. (2) Oversized packets. (3) Interface congestion. (4) Loopback packets sent on non loop back interface.

NIC hangs (Hangs) Number of times the specified interface detected hangs in the transmit and receive paths since the Citrix ADC was started or the interface statistics were cleared.

Status stalls (StsStall) Number of times the status updates for a specified interface were stalled since the Citrix ADC was started or the interface statistics were cleared. A status stall is detected when the status of the interface is not updated by the NIC hardware within 0.8 seconds of the last update.

Transmit stalls (TxStall) Number of times the interface stalled, when transmitting packets, since the Citrix ADC was started or the interface statistics were cleared. Transmit (Tx) stalls are detected when a packet posted for transmission is not transmitted in 4 seconds.

Receive stalls (RxStall) Number of times the interface stalled, when receiving packets, since the Citrix ADC was started or the interface statistics were cleared. Receive (Rx) stalls are detected when the following conditions are met: (1)The link is up for more than 10 minutes. (2)Packets are transmitted, but no packets is received for 16 seconds.

Error-disables (ErrDis) Number of times the specified interface is disabled by the Citrix ADC, due to continuous Receive (Rx) or Transmit (Tx) stalls, since the Citrix ADC was started or the interface statistics were cleared. The Citrix ADC disables an interface when one of the following conditions is met: (1) Three consecutive transmit stalls occurs with at most gap of 10 seconds between any two stalls. (2) Three consecutive receive stalls occurs with at most gap of 120 seconds between any two stalls.

Link re-initializations (LnkReint) Number of times the link has been re-initialized. A re-initialization occurs due to link state change, configuration parameter change, or administrative reset operation.

MAC moves registered (MacMvd) Number of MAC moves between ports. If a high rate of MAC moves is observed, it is likely that there is a bridge loop between two interfaces.

Times NIC became muted (ErrMtd) Number of times the specified interface stopped transmitting and receiving packets due to MAC moves between ports.

Receive CRC errors (ErrRxCRC) Number of packets received with the wrong checksum by the specified interface since the Citrix ADC was started or the interface statistics were cleared. This indicates the number of Jabber frames received instead of CRC errors on the 10G data ports of Citrix ADC 12000-10G platform and the data ports of Citrix ADC MPX 15000 and 17000 platforms.

Interface Alias (IntfAlias) Alias Name for the Interface

Link State (State) The current state of the link associated with the interface. For logical interfaces (LA), the state of the link is dependent on the state of the slave interfaces. For the link to be UP at least one of the slave interfaces needs to be UP.

Related Commands

- stat MapDomain

disable interface

Disables the interface from transmitting and receiving packets. The link remains active and the peer network device is unaware that the interface has been disabled. In a High Availability configuration, an interface that has HA MON enabled and is not bound to any Failover Interface Set (FIS), is a critical interface. Disabling or failure of any critical interface triggers HA failover.

Note: To view the status of an interface, use the show interface command.

Synopsis

disable interface <id>@

Arguments

id Interface number, in C/U format, where C can take one of the following values:

- 0 - Indicates a management interface.
- 1 - Indicates a 1 Gbps port.
- 10 - Indicates a 10 Gbps port.
- LA - Indicates a link aggregation port.
- LO - Indicates a loop back port. U is a unique integer for representing an interface in a particular port group.

interfacePair

The following operations can be performed on "interfacePair":

add| show| rm|

add interfacePair

Create an Interface Pair. Each Interface Pair or IFPAIR is identified by a IFID (integer from 1-255).

Synopsis

add interfacePair <id> -ifnum <interface_name> ...

Arguments

id The Interface pair id Minimum value: 1 Maximum value: 255

ifnum The constituent interfaces in the interface pair Minimum value: 1

show interfacePair

Displays the configured Interface Pairs. If id is specified, then only that particular IFPAIR information is displayed. If it is not specified, all configured IFPAIRs are displayed.

Synopsis

show interfacePair

Arguments

id The Interface pair id Minimum value: 1 Maximum value: 255

Output

ifnum The constituent interfaces in the interface pair

ifaces Names of all member interfaces of this Interface Pair

stateflag state flag

devno count

Example

An example of the output of the show interfacepair command is as follows:

1. ```
   IFPAIR ID: 3

   Member Interfaces : 1/4 1/3
   ```

2. ```
   IFPAIR ID: 4

   Member Interfaces : 1/6 1/5
   ```

Done

rm interfacePair

Removes the IFPAIR created by the add intfPair command. Once the IFPAIR is removed, its interfaces become independent.

Synopsis

rm interfacePair <id>

Arguments

id The Interface pair id Minimum value: 1 Maximum value: 255

ip6Tunnel

The following operations can be performed on "ip6Tunnel":

add| show| rm|

add ip6Tunnel

Creates an IPv6 tunnel. An IP tunnel is a communication channel, using encapsulation technologies, between two networks that do not have a routing path. Every IP packet that is shared between the two networks is encapsulated within another packet and then sent through the tunnel.

Synopsis

add ip6Tunnel <name> <remote> <local>

Arguments

name Name for the IPv6 Tunnel. Cannot be changed after the service group is created. Must begin with a number or letter, and can consist of letters, numbers, and the @ _ - . (period) : (colon) # and space ( ) characters.

remote An IPv6 address of the remote Citrix ADC used to set up the tunnel.

local An IPv6 address of the local Citrix ADC used to set up the tunnel.

ownerGroup The owner node group in a Cluster for the tunnel. Default value: DEFAULT_NG

Example

add ip6tunnel tun6 9901::200/64 *

Related Commands

- set ip6tunnelParam

show ip6Tunnel

Displays the settings of all IPv6 tunnels configured on the Citrix ADC, or of the specified IPv6 tunnel.

Synopsis

show ip6Tunnel

Arguments

name Name of the IPv6 tunnel whose details you want to display.

remote The IPv6 address at which the remote Citrix ADC connects to the tunnel.

Output

remoteIP The remote IP address or subnet of the tunnel.

local An IPv6 address of the local Citrix ADC used to set up the tunnel.

type The type of this tunnel.

encapIp The effective local IP address of the tunnel. Used as the source of the encapsulated packets.

ownerGroup The owner node group in a Cluster for the tunnel.

devno count stateflag

Example

1. Name.....: tun61 Remote.....: 9901::200/64 Local.....: * Encap.....: ::0/128 Type.....: C
2. Name.....: tun62 Remote.....: 9903::400/84 Local.....: 9903::100 Encap.....: ::0/128 Type.....: C
3. Name.....: Remote.....: 9902::300/90 Local.....: * Encap.....: 9902::100 Type.....: I

Related Commands

- show ip6tunnelParam

rm ip6Tunnel

Removes an IPv6 tunnel from the Citrix ADC.

Synopsis

rm ip6Tunnel <name>

Arguments

name Name of the IPv6 tunnel to be removed.

Example

rm ip6tunnel tun6

Related Commands

- show ip6tunnelParam

ip6TunnelParam

The following operations can be performed on "ip6TunnelParam":

set| unset| show|

set ip6TunnelParam

Sets global parameters of IPv6 tunnels on the Citrix ADC.

Synopsis

set ip6TunnelParam

Arguments

srcIP Common source IPv6 address for all IPv6 tunnels. Must be a SNIP6 or VIP6 address.

dropFrag Drop any packet that requires fragmentation.

Possible values: YES, NO Default value: NO

dropFragCpuThreshold Threshold value, as a percentage of CPU usage, at which to drop packets that require fragmentation. Applies only if dropFragparameter is set to NO. Minimum value: 1 Maximum value: 100

srcIPRoundRobin Use a different source IPv6 address for each new session through a particular IPv6 tunnel, as determined by round robin selection of one of the SNIP6 addresses. This setting is ignored if a common global source IPv6 address has been specified for all the IPv6 tunnels. This setting does not apply to a tunnel for which a source IPv6 address has been specified.

Possible values: YES, NO Default value: NO

useClientSourceIPv6 Use client source IPv6 address as source IPv6 address for outer tunnel IPv6 header

Possible values: YES, NO Default value: NO

Example

set ip6TunnelParam -srcIP 9901::100 -dropFrag YES -dropFragCpuThreshold 95 -useClientSourceIPv6 YES

Related Commands

- show ip6tunnel

unset ip6TunnelParam

Resets the specified global parameters of IPv6 tunnels to their default settings. Refer to the set ip6TunnelParam command for parameter descriptions..Refer to the set ip6TunnelParam command for meanings of the arguments.

Synopsis

unset ip6TunnelParam

Example

unset ip6TunnelParam -srcIP -dropFrag -dropFragCpuThreshold -useClientSourceIPv6

Related Commands

- show ip6tunnel

show ip6TunnelParam

Displays the global settings of IPv6 tunnels on the Citrix ADC.

Synopsis

show ip6TunnelParam

Arguments

Output

srcIP Common source IPv6 address for all IPv6 tunnels. Must be a SNIP6 or VIP6 address.

dropFrag Drop any packet that requires fragmentation.

dropFragCpuThreshold Threshold value, as a percentage of CPU usage, at which to drop packets that require fragmentation. Applies only if dropFragparameter is set to NO.

srcIPRoundRobin Use a different source IPv6 address for each new session through a particular IPv6 tunnel, as determined by round robin selection of one of the SNIP6 addresses. This setting is ignored if a common global source IPv6 address has been specified for all the IPv6 tunnels. This setting does not apply to a tunnel for which a source IPv6 address has been specified.

useClientSourceIPv6 Use client source IPv6 address as source IPv6 address for outer tunnel IPv6 header

Example

Tunnel Source IP: 9901::100 Round Robin of Tunnel Source IP: NO Drop if Fragmentation Needed: YES CPU usage threshold to avoid fragmentation: 95 Use client sourceIP6 as sourceIP6 for outer tunnel IP6 header: YES

Related Commands

- show ip6tunnel

ipTunnel

The following operations can be performed on "ipTunnel":

add| set| rm| show| unset|

add ipTunnel

Creates an IPv4 tunnel. An IP tunnel is a communication channel, using encapsulation technologies, between two networks that do not have a routing path. Every IP packet that is shared between the two networks is encapsulated within another packet and then sent through the tunnel.

Synopsis

add ipTunnel <name> <remote> <remoteSubnetMask> <local>

Arguments

name Name for the IP tunnel. Leading character must be a number or letter. Other characters allowed, after the first character, are @ _ - . (period) : (colon) # and space ( ).

remote Public IPv4 address, of the remote device, used to set up the tunnel. For this parameter, you can alternatively specify a network address.

remoteSubnetMask Subnet mask of the remote IP address of the tunnel.

local Type of Citrix ADC owned public IPv4 address, configured on the local Citrix ADC and used to set up the tunnel.

protocol Name of the protocol to be used on this tunnel.

Possible values: IPIP, GRE, IPSEC, UDP, GENEVE Default value: IPIP

vnid Virtual network identifier (VNID) is the value that identifies a specific virtual network in the data plane. Minimum value: 1 Maximum value: 16777215

vlanTagging Option to select Vlan Tagging.

Possible values: ENABLED, DISABLED Default value: DISABLED

destPort Specifies UDP destination port for Geneve packets. Default port is 6081. Default value: 6081 Minimum value: 1024 Maximum value: 65535

tosInherit Default behavior is to copy the ToS field of the internal IP Packet (Payload) to the outer IP packet (Transport packet). But the user can configure a new ToS field using this option.

Possible values: ENABLED, DISABLED Default value: ENABLED

grepayload The payload GRE will carry

Possible values: ETHERNETwithDOT1Q, ETHERNET, IP Default value: ETHERNETwithDOT1Q

ipsecProfileName Name of IPSec profile to be associated. Default value: "ns_ipsec_default_profile"

vlan The vlan for mulicast packets Minimum value: 1 Maximum value: 4094

ownerGroup The owner node group in a Cluster for the iptunnel. Default value: DEFAULT_NG

Example

add iptunnel tunnel1 10.100.20.0 255.255.255.0 *

Related Commands

- set iptunnelParam

set ipTunnel

Modifies parameters of a GENEVE Tunnel.

Synopsis

set ipTunnel <name>

Arguments

name Name of the IP tunnel

vlanTagging Enable or disable the VlanTagging in a Geneve Tunnel.

Possible values: ENABLED, DISABLED Default value: DISABLED

destPort Change the detination port for a Geneve Tunnel. Default value: 6081 Minimum value: 1024 Maximum value: 65535

tosInherit Enable or disable the copying of ToS value from the inner packet to the outer IP packet.

Possible values: ENABLED, DISABLED Default value: ENABLED

Example

set iptunnel tun1 -destPort 2000 -tosInherit DISABLED -vlanTagging DISABLED

rm ipTunnel

Removes an IP tunnel configuration from the Citrix ADC.

Synopsis

rm ipTunnel <name>

Arguments

name Name of the IP Tunnel.

Example

rm iptunnel tunnel1

Related Commands

- show iptunnelParam

show ipTunnel

Display the configured IP tunnels.

Synopsis

show ipTunnel

Arguments

remote Public IPv4 address, of the remote device, used to set up the tunnel. For this parameter, you can alternatively specify a network address.

remoteSubnetMask Subnet mask of the remote IP address of the tunnel.

name Name for the IP tunnel. Leading character must be a number or letter. Other characters allowed, after the first character, are @ _ - . (period) : (colon) # and space ( ).

Output

name The name of the ip tunnel.

local Type of Citrix ADC owned public IPv4 address, configured on the local Citrix ADC and used to set up the tunnel.

protocol Name of the protocol to be used on this tunnel.

grepayload The payload GRE will carry

type The type of this tunnel.

encapIp The effective local IP address of the tunnel. Used as the source of the encapsulated packets.

channel The tunnel that is bound to a netbridge.

ipsecProfileName Name of IPSec profile to be associated.

vlan The vlan for mulicast packets

tunnelType Indicates that a tunnel is User-Configured, Internal or DELETE-IN-PROGRESS.

ipsecTunnelStatus Whether the ipsec on this tunnel is up or down.

ownerGroup The owner node group in a Cluster for the iptunnel.

refcnt Number of PBRs to bound to this iptunnel

vnid Virtual network identifier (VNID) is the value that identifies a specific virtual network in the data plane.

vlanTagging Option to select Vlan Tagging.

destPort Specifies UDP destination port for Geneve packets. Default port is 6081.

tosInherit Default behavior is to copy the ToS field of the internal IP Packet (Payload) to the outer IP packet (Transport packet). But the user can configure a new ToS field using this option.

devno count stateflag

Example

1. Name.....: t1 Remote.....: 10.102.33.0 Mask.....: 255.255.255.0 Local.....: * Encap.....: 0.0.0.0 Protocol.....: IPIP Type.....: C
2. Name.....: tunnel1 Remote.....: 10.100.20.0 Mask.....: 255.255.255.0 Local.....: * Encap.....: 0.0.0.0 Protocol.....: IPIP Type.....: C
3. Name.....: Remote.....: 10.102.33.190 Mask.....: 255.255.255.255 Local.....: * Encap.....: 10.102.33.85 Protocol.....: IPIP Type.....: I

Related Commands

- show iptunnelParam

unset ipTunnel

Use this command to remove ipTunnel settings.Refer to the set ipTunnel command for meanings of the arguments.

Synopsis

unset ipTunnel <name>

ipTunnelParam

The following operations can be performed on "ipTunnelParam":

show| set| unset|

show ipTunnelParam

Display the IP Tunnel global settings on the Citrix ADC

Synopsis

show ipTunnelParam

Arguments

Output

srcIP Common source-IP address for all tunnels. For a specific tunnel, this global setting is overridden if you have specified another source IP address. Must be a MIP or SNIP address.

dropFrag Drop any IP packet that requires fragmentation before it is sent through the tunnel.

dropFragCpuThreshold Threshold value, as a percentage of CPU usage, at which to drop packets that require fragmentation to use the IP tunnel. Applies only if dropFragparameter is set to NO. The default value, 0, specifies that this parameter is not set.

srcIPRoundRobin Use a different source IP address for each new session through a particular IP tunnel, as determined by round robin selection of one of the SNIP addresses. This setting is ignored if a common global source IP address has been specified for all the IP tunnels. This setting does not apply to a tunnel for which a source IP address has been specified.

enableStrictRx Strict PBR check for IPSec packets received through tunnel

enableStrictTx Strict PBR check for packets to be sent IPSec protected

mac The shared MAC used for shared IP between cluster nodes/HA peers

useClientSourceIP Use client source IP as source IP for outer tunnel IP header

Example

Tunnel Source IP: 10.100.20.48 Round Robin of Tunnel Source IP: NO Drop if Fragmentation Needed: NO CPU usage threshold to avoid fragmentation: 95 Strict PBR check for IPSec packets received through tunnel: NO Strict PBR check for packets to be sent IPSec protected: NO Tunnel MAC for shared IPs: 00:00:00:00:00:00 Use client sourceIP as sourceIP for outer tunnel IP header: YES

Related Commands

- show iptunnel

set ipTunnelParam

Sets global parameters of IPv4 tunnels on the Citrix ADC.

Synopsis

set ipTunnelParam

Arguments

srcIP Common source-IP address for all tunnels. For a specific tunnel, this global setting is overridden if you have specified another source IP address. Must be a MIP or SNIP address.

dropFrag Drop any IP packet that requires fragmentation before it is sent through the tunnel.

Possible values: YES, NO Default value: NO

dropFragCpuThreshold Threshold value, as a percentage of CPU usage, at which to drop packets that require fragmentation to use the IP tunnel. Applies only if dropFragparameter is set to NO. The default value, 0, specifies that this parameter is not set. Minimum value: 1 Maximum value: 100

srcIPRoundRobin Use a different source IP address for each new session through a particular IP tunnel, as determined by round robin selection of one of the SNIP addresses. This setting is ignored if a common global source IP address has been specified for all the IP tunnels. This setting does not apply to a tunnel for which a source IP address has been specified.

Possible values: YES, NO Default value: NO

enableStrictRx Strict PBR check for IPSec packets received through tunnel

Possible values: YES, NO Default value: NO

enableStrictTx Strict PBR check for packets to be sent IPSec protected

Possible values: YES, NO Default value: NO

mac The shared MAC used for shared IP between cluster nodes/HA peers

useClientSourceIP Use client source IP as source IP for outer tunnel IP header

Possible values: YES, NO Default value: NO

Example

set ipTunnelParam -srcIP 10.100.20.48 -dropFrag YES -dropFragCpuThreshold 95 -useClientSourceIP YES

Related Commands

- show iptunnel

unset ipTunnelParam

Use this command to remove ipTunnelParam settings.Refer to the set ipTunnelParam command for meanings of the arguments.

Synopsis

unset ipTunnelParam

ipset

The following operations can be performed on "ipset":

rm| show| unbind| add| bind|

rm ipset

Removes an IP set from the Citrix ADC.

Synopsis

rm ipset <name> ...

Arguments

name Name of the IP set to be removed.

Example

rm ipset pool1

show ipset

Displays the settings of all IP sets configured on the Citrix ADC, or of the specified IP set.

Synopsis

show ipset

Arguments

name Name of the IP set whose details you want to display.

Output

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

IPAddress One or more IP addresses bound to the IP set.

stateflag state flag

flags ipSetRefcount Used to keep reference count of IP

devno count

Example

show network ipset

unbind ipset

Unbinds the associated IP addresses from an IP set.

Synopsis

unbind ipset <name> <IPAddress>@ ...

Arguments

name Name of the IP set from which to unbind IP addresses.

IPAddress IP addresses to be unbound from the IP set. (If using the CLI, use spaces to separate multiple addresses.)

Example

unbind ipset ipset_1 10.102.1.10

add ipset

Creates an IP set to which you can bind subnet IP (SNIP) or mapped IP (MIP) addresses that have been configured on the Citrix ADC.

Synopsis

add ipset <name>

Arguments

name Name for the IP set. Must begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the IP set is created. Choose a name that helps identify the IP set.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

Example

add ipset pool1

bind ipset

Binds specified IP addresses to an IP set.

Synopsis

bind ipset <name> <IPAddress>@ ...

Arguments

name Name of the IP set to which to bind IP addresses.

IPAddress SNIP or MIP addresses, configured on the Citrix ADC, to be bound to the IP set. (If using the CLI, use spaces to separate multiple addresses.)

Example

bind ipset ipset_1 10.102.1.10

ipv6

The following operations can be performed on "ipv6":

unset| set| show|

unset ipv6

Unset the IPv6-related parameters: RA Learning and IPv6 NAT Prefix..Refer to the set ipv6 command for meanings of the arguments.

Synopsis

unset ipv6 [-natprefix]

Example

unset ipv6 -natprefix -td 1

set ipv6

Sets the IPv6-related parameters.

Synopsis

set ipv6 [-natprefix <ipv6_addr|*>]

Arguments

ralearning Enable the Citrix ADC to learn about various routes from Router Advertisement (RA) and Router Solicitation (RS) messages sent by the routers.

Possible values: ENABLED, DISABLED Default value: DISABLED

routerRedirection Enable the Citrix ADC to do Router Redirection.

Possible values: ENABLED, DISABLED Default value: DISABLED

ndBasereachTime Base reachable time of the Neighbor Discovery (ND6) protocol. The time, in milliseconds, that the Citrix ADC assumes an adjacent device is reachable after receiving a reachability confirmation. Default value: 30000 Minimum value: 1

ndRetransmissionTime Retransmission time of the Neighbor Discovery (ND6) protocol. The time, in milliseconds, between retransmitted Neighbor Solicitation (NS) messages, to an adjacent device. Default value: 1000 Minimum value: 1

natprefix Prefix used for translating packets from private IPv6 servers to IPv4 packets. This prefix has a length of 96 bits (128-32 = 96). The IPv6 servers embed the destination IP address of the IPv4 servers or hosts in the last 32 bits of the destination IP address field of the IPv6 packets. The first 96 bits of the destination IP address field are set as the IPv6 NAT prefix. IPv6 packets addressed to this prefix have to be routed to the Citrix ADC to ensure that the IPv6-IPv4 translation is done by the appliance.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Default value: 0 Minimum value: 0 Maximum value: 4094

doDAD Enable the Citrix ADC to do Duplicate Address Detection (DAD) for all the Citrix ADC owned IPv6 addresses regardless of whether they are obtained through stateless auto configuration, DHCPv6, or manual configuration.

Possible values: ENABLED, DISABLED Default value: DISABLED

usipnatprefix IPV6 NATPREFIX used in NAT46 scenario when USIP is turned on

Example

set ipv6 -natprefix 2000::/96

show ipv6

Display IPv6 settings

Synopsis

show ipv6

Arguments

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Default value: 0 Minimum value: 0 Maximum value: 4094

Output

ralearning Enable the Citrix ADC to learn about various routes from Router Advertisement (RA) and Router Solicitation (RS) messages sent by the routers.

routerRedirection Enable the Citrix ADC to do Router Redirection.

basereachtime ND6 base reachable time (ms)

ndBasereachTime Base reachable time of the Neighbor Discovery (ND6) protocol. The time, in milliseconds, that the Citrix ADC assumes an adjacent device is reachable after receiving a reachability confirmation.

reachtime ND6 computed reachable time (ms)

ndreachtime ND6 computed reachable time (ms)

retransmissiontime ND6 retransmission time (ms)

ndRetransmissionTime Retransmission time of the Neighbor Discovery (ND6) protocol. The time, in milliseconds, between retransmitted Neighbor Solicitation (NS) messages, to an adjacent device.

natprefix Prefix used for translating packets from private IPv6 servers to IPv4 packets. This prefix has a length of 96 bits (128-32 = 96). The IPv6 servers embed the destination IP address of the IPv4 servers or hosts in the last 32 bits of the destination IP address field of the IPv6 packets. The first 96 bits of the destination IP address field are set as the IPv6 NAT prefix. IPv6 packets addressed to this prefix have to be routed to the Citrix ADC to ensure that the IPv6-IPv4 translation is done by the appliance.

doDAD Enable the Citrix ADC to do Duplicate Address Detection (DAD) for all the Citrix ADC owned IPv6 addresses regardless of whether they are obtained through stateless auto configuration, DHCPv6, or manual configuration.

usipnatprefix IPV6 NATPREFIX used in NAT46 scenario when USIP is turned on

devno count stateflag

Example

show ipv6

lacp

The following operations can be performed on "lacp":

show| set|

show lacp

Displays the settings of all channels created by the link aggregation control protocol (LACP) on the Citrix ADC.

Synopsis

show lacp

Arguments

ownerNode The owner node in a cluster for which we want to set the lacp priority. Owner node can vary from 0 to 31. Ownernode value of 254 is used for Cluster. Default value: 255 Minimum value: 0

Output

deviceName Name of the channel.

sysPriority Priority number that determines which peer device of an LACP LA channel can have control over the LA channel. This parameter is globally applied to all LACP channels on the Citrix ADC. The lower the number, the higher the priority.

mac LACP system MAC.

flags Flags of this channel.

lacpKey LACP key of this channel.

clustersysPriority LACP system (Cluster) priority

clusterMac LACP system (Cluster) mac.

devno count stateflag

set lacp

Sets the Link Aggregation Control Protocol (LACP) system priority. Note: The Citrix ADC automatically adds a parameter called mac in the configuration file (ns.conf) for this command entry. This parameter is set to the MAC address of one of the Citrix ADC appliance's interfaces and is used along with the system priority to form the system ID for the LACP channel.

Synopsis

set lacp -sysPriority <positive_integer>

Arguments

sysPriority Priority number that determines which peer device of an LACP LA channel can have control over the LA channel. This parameter is globally applied to all LACP channels on the Citrix ADC. The lower the number, the higher the priority. Default value: 32768 Minimum value: 1 Maximum value: 65535

ownerNode The owner node in a cluster for which we want to set the lacp priority. Owner node can vary from 0 to 31. Ownernode value of 254 is used for Cluster. Default value: 255 Minimum value: 0

linkset

The following operations can be performed on "linkset":

bind| unbind| rm| show| add|

bind linkset

Binds interfaces to the linkset.

Synopsis

bind linkset <id> -ifnum <interface_name> ...

Arguments

id ID of the linkset to which to bind the interfaces.

ifnum The interfaces to be bound to the linkset.

Example

bind linkset LS/1 -ifnum 1/1/1

unbind linkset

Unbinds interfaces from the linkset.

Synopsis

unbind linkset <id> -ifnum <interface_name> ...

Arguments

id ID of the linkset from which to unbind the interfaces.

ifnum Interfaces to be unbound from the linkset.

Example

unbind linkset LS/1 -ifnum 1/1/1

rm linkset

Removes a linkset from the cluster.

Synopsis

rm linkset <id>

Arguments

id ID of the linkset to be removed.

Example

rm linkset LS/1

show linkset

Displays information about all linksets, or displays information about the specified linkset.

Synopsis

show linkset

Arguments

id ID of the linkset for which to display information. If an ID is not provided, the display includes information about all linksets that are available in the cluster.

Output

ifnum The interfaces to be bound to the linkset.

stateflag state flag

devno count

Example

show linkset

add linkset

Adds a linkset to the Citrix ADC cluster.

Synopsis

add linkset <id>

Arguments

id Unique identifier for the linkset. Must be of the form LS/x, where x can be an integer from 1 to 32.

Example

add linkset LS/1

nat64

The following operations can be performed on "nat64":

rm| set| stat| unset| add| show|

rm nat64

Remove the configured nat64 rule.

Synopsis

rm nat64 <name>

Arguments

name Name for the NAT64 rule. Must begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the rule is created. Choose a name that helps identify the NAT64 rule.

Example

rm nat64 name.

set nat64

Set the configured nat64 rule.

Synopsis

set nat64 <name>

Arguments

name Name for the NAT64 rule. Must begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the rule is created. Choose a name that helps identify the NAT64 rule.

acl6name Name of any configured ACL6 whose action is ALLOW. IPv6 Packets matching the condition of this ACL6 rule and destination IP address of these packets matching the NAT64 IPv6 prefix are considered for NAT64 translation.

netProfile Name of the configured netprofile. The Citrix ADC selects one of the IP address in the netprofile as the source IP address of the translated IPv4 packet to be sent to the IPv4 server.

Example

set nat64 rule1 -acl6name acl1 .

stat nat64

Display statistics for nat64 sessions.

Synopsis

stat nat64

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

TCP Sessions (nat64TotTcpSessions) Total number of TCP sessions created by NAT64.

UDP Sessions (nat64TotUdpSessions) Total number of UDP sessions created by NAT64.

ICMP Sessions (nat64TotIcmpSessions) Total number of ICMP sessions created by NAT64.

Total Sessions (nat64TotSessions) Total number of sessions created by NAT64.

Example

stat nat64

Related Commands

- stat MapDomain

unset nat64

Use this command to remove nat64 settings.Refer to the set nat64 command for meanings of the arguments.

Synopsis

unset nat64 <name> -netProfile

add nat64

Configure a nat64 rule on the appliance.

Synopsis

add nat64 <name> <acl6name>

Arguments

name Name for the NAT64 rule. Must begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the rule is created. Choose a name that helps identify the NAT64 rule.

acl6name Name of any configured ACL6 whose action is ALLOW. IPv6 Packets matching the condition of this ACL6 rule and destination IP address of these packets matching the NAT64 IPv6 prefix are considered for NAT64 translation.

netProfile Name of the configured netprofile. The Citrix ADC selects one of the IP address in the netprofile as the source IP address of the translated IPv4 packet to be sent to the IPv4 server.

show nat64

Display the nat64 configuration.

Synopsis

show nat64

Arguments

name Name for the NAT64 rule. Must begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the rule is created. Choose a name that helps identify the NAT64 rule.

Output

acl6name Name of any configured ACL6 whose action is ALLOW. IPv6 Packets matching the condition of this ACL6 rule and destination IP address of these packets matching the NAT64 IPv6 prefix are considered for NAT64 translation.

netProfile Name of the configured netprofile. The Citrix ADC selects one of the IP address in the netprofile as the source IP address of the translated IPv4 packet to be sent to the IPv4 server.

devno count stateflag

nat64param

The following operations can be performed on "nat64param":

unset| show| set|

unset nat64param

Use this command to remove nat64param settings.Refer to the set nat64param command for meanings of the arguments.

Synopsis

unset nat64param

show nat64param

Show the nat64 parameters.

Synopsis

show nat64param

Arguments

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Default value: 0 Minimum value: 0 Maximum value: 4094

Output

nat64IgnoreTOS Ignore TOS.

nat64ZeroCheckSum Calculate checksum for UDP packets with zero checksum

nat64v6Mtu MTU setting for the IPv6 side. If the incoming IPv4 packet greater than this, either fragment or send icmp need fragmentation error.

nat64FragHeader When disabled, translator will not insert IPv6 fragmentation header for non fragmented IPv4 packets

devno count stateflag

Example

show nat64param

set nat64param

Set the nat64 parameter

Synopsis

set nat64param

Arguments

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Default value: 0 Minimum value: 0 Maximum value: 4094

nat64IgnoreTOS Ignore TOS.

Possible values: YES, NO Default value: NO

nat64ZeroCheckSum Calculate checksum for UDP packets with zero checksum

Possible values: ENABLED, DISABLED Default value: ENABLED

nat64v6Mtu MTU setting for the IPv6 side. If the incoming IPv4 packet greater than this, either fragment or send icmp need fragmentation error. Default value: 1280 Minimum value: 1280 Maximum value: 9216

nat64FragHeader When disabled, translator will not insert IPv6 fragmentation header for non fragmented IPv4 packets

Possible values: ENABLED, DISABLED Default value: ENABLED

Example

set nat64param -nat64ignoretos YES

nd6

The following operations can be performed on "nd6":

add| show| clear| rm|

add nd6

Adds a static entry to the ND6 table of the Citrix ADC.

Synopsis

add nd6 <neighbor> <mac> (<ifnum> | -vxlan <positive_integer>)

Arguments

neighbor Link-local IPv6 address of the adjacent network device to add to the ND6 table.

mac MAC address of the adjacent network device.

ifnum Interface through which the adjacent network device is available, specified in slot/port notation (for example, 1/3). Use spaces to separate multiple entries.

vlan Integer value that uniquely identifies the VLAN on which the adjacent network device exists. Minimum value: 1 Maximum value: 4094

vxlan ID of the VXLAN on which the IPv6 address of this ND6 entry is reachable. Minimum value: 1 Maximum value: 16777215

vtep IP address of the VXLAN tunnel endpoint (VTEP) through which the IPv6 address of this ND6 entry is reachable.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

Example

add nd6 2001::1 00:04:23:be:3c:06 5 1/1

show nd6

Display the neighbor discovery information.

Synopsis

show nd6 [<neighbor>]

Arguments

neighbor Link-local IPv6 address of the adjacent network device to add to the ND6 table.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

Output

mac MAC address of the adjacent network device.

state ND6 state

timeout Time elapsed

ifnum Interface through which the adjacent network device is available, specified in slot/port notation (for example, 1/3). Use spaces to separate multiple entries.

vlan Integer value that uniquely identifies the VLAN on which the adjacent network device exists.

vxlan ID of the VXLAN on which the IPv6 address of this ND6 entry is reachable.

vtep IP address of the VXLAN tunnel endpoint (VTEP) through which the IPv6 address of this ND6 entry is reachable.

flags flag for static/permanent entry.

controlPlane This nd6 entry is populated by a control plane protocol

channel The tunnel that is bound to a netbridge.

devno count stateflag

Example

Following is an example of the output for the show nd6 command:

Neighbor MAC-Address(Vlan, Interface) State TIME(hh:mm:ss)

2001::1 00:04:23:be:3c:06(5, 1/1) REACHABLE 00:00:24 FE80::123:1 00:04:23:be:3c:07(4, 1/2) STALE 00:03:34

clear nd6

Removes all IPv6 neighbour discovery entries from the Citrix ADC.

Synopsis

clear nd6

Arguments

rm nd6

Remove a static IPv6 neighbor discovery entry from the Citrix ADC's ND6 table.

Synopsis

rm nd6 <neighbor>

Arguments

neighbor Link-local IPv6 address of the adjacent network device that you want to remove from the ND6 table.

vlan Integer value that uniquely identifies the VLAN for the ND6 entry you want to remove. Minimum value: 1 Maximum value: 4094

vxlan Integer value that uniquely identifies the VXLAN for the ND6 entry you want to remove. Minimum value: 1 Maximum value: 16777215

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

Example

rm nd6 2001::1 5 1/1

nd6RAvariables

The following operations can be performed on "nd6RAvariables":

bind| unbind| unset| set| show|

bind nd6RAvariables

Bind on-link global prefixes to Router Advertisments variables.

Synopsis

bind nd6RAvariables -vlan <positive_integer> -ipv6Prefix <ipv6_addr|*>

Arguments

vlan The VLAN number. Minimum value: 1 Maximum value: 4094

ipv6Prefix Onlink prefixes for RA messages.

Example

bind nd6RAvariables -vlan 2 -ipv6Prefix 8000::/64

unbind nd6RAvariables

Unbind prefix from Router Advertisment parameters in Citrix ADC

Synopsis

unbind nd6RAvariables -vlan <positive_integer> -ipv6Prefix <ipv6_addr|*>

Arguments

vlan The VLAN number. Minimum value: 1 Maximum value: 4094

ipv6Prefix Onlink prefixes for RA messages.

Example

unbind nd6RAvariables -vlan 2 -ipv6Prefix 8000::/64

unset nd6RAvariables

Use this command to remove nd6RAvariables settings.Refer to the set nd6RAvariables command for meanings of the arguments.

Synopsis

unset nd6RAvariables -vlan <positive_integer>

set nd6RAvariables

Set vlan specific Router Advertisment parameters in Citrix ADC.

Synopsis

set nd6RAvariables -vlan <positive_integer>

Arguments

vlan The VLAN number. Minimum value: 1 Maximum value: 4094

ceaseRouterAdv Cease router advertisements on this vlan.

Possible values: YES, NO Default value: NO

sendRouterAdv whether the router sends periodic RAs and responds to Router Solicitations.

Possible values: YES, NO Default value: NO

srcLinkLayerAddrOption Include source link layer address option in RA messages.

Possible values: YES, NO Default value: YES

onlyUnicastRtAdvResponse Send only Unicast Router Advertisements in respond to Router Solicitations.

Possible values: YES, NO Default value: NO

managedAddrConfig Value to be placed in the Managed address configuration flag field.

Possible values: YES, NO Default value: NO

otherAddrConfig Value to be placed in the Other configuration flag field.

Possible values: YES, NO Default value: NO

currHopLimit Current Hop limit. Default value: 64 Minimum value: 0 Maximum value: 255

maxRtAdvInterval Maximum time allowed between unsolicited multicast RAs, in seconds. Default value: 600 Minimum value: 4 Maximum value: 1800

minRtAdvInterval Minimum time interval between RA messages, in seconds. Default value: 198 Minimum value: 3 Maximum value: 1350

linkMTU The Link MTU. Default value: 0 Minimum value: 0 Maximum value: 1500

reachableTime Reachable time, in milliseconds. Default value: 0 Minimum value: 0 Maximum value: 3600000

retransTime Retransmission time, in milliseconds. Default value: 0 Minimum value: 0

defaultLifeTime Default life time, in seconds. Default value: 1800 Minimum value: 0 Maximum value: 9000

Example

set nd6RAvariables -vlan 2 -maxRtAdvInterval 600

show nd6RAvariables

Display Router Advertisement configuration variables.

Synopsis

show nd6RAvariables

Arguments

vlan The VLAN number. Minimum value: 1 Maximum value: 4094

Output

ceaseRouterAdv Cease router advertisements on this vlan.

sendRouterAdv whether the router sends periodic RAs and responds to Router Solicitations.

srcLinkLayerAddrOption Include source link layer address option in RA messages.

onlyUnicastRtAdvResponse Send only Unicast Router Advertisements in respond to Router Solicitations.

managedAddrConfig Value to be placed in the Managed address configuration flag field.

otherAddrConfig Value to be placed in the Other configuration flag field.

currHopLimit Current Hop limit.

maxRtAdvInterval Maximum time allowed between unsolicited multicast RAs, in seconds.

minRtAdvInterval Minimum time interval between RA messages, in seconds.

linkMTU The Link MTU.

reachableTime Reachable time, in milliseconds.

retransTime Retransmission time, in milliseconds.

defaultLifeTime Default life time, in seconds.

stateflag RA Param state flags.

lastRtAdvTime Last RA sent timestamp.

nextRtAdvDelay Next RA delay.

ipv6Prefix Onlink prefixes for RA messages.

devno count

netProfile

The following operations can be performed on "netProfile":

unset| unbind| bind| set| add| rm| show|

unset netProfile

Removes the srcIP attribute of a net profile..Refer to the set netProfile command for meanings of the arguments.

Synopsis

unset netProfile <name>

Example

unset netProfile prof1 -srcIP

unbind netProfile

Unbinds the specified port range from a netprofile.

Synopsis

unbind netProfile <name> (-srcPortRange <int> ... | (-natRule <ip_addr> <netmask>))

Arguments

name Name of the netprofile to which to bind port ranges.

srcPortRange When the source port range is configured and associated with the netprofile bound to a service group, Citrix ADC will choose a port from the range configured for connection establishment at the backend servers. Minimum value: 1024 Maximum value: 65535

natRule Unbind the already bound natrule from netProfile.

netmask

Example

unbind netprofile npf_1 -srcportrange 2000-3000 unbind netprofile npf_1 -natrule 1.0.0.0 255.0.0.0

bind netProfile

Binds specified port range to a netprofile.

Synopsis

bind netProfile <name> (-srcPortRange <int> ... | (-natRule <ip_addr> <netmask> <rewriteIp>))

Arguments

name Name of the netprofile to which to bind port ranges.

srcPortRange When the source port range is configured and associated with the netprofile bound to a service group, Citrix ADC will choose a port from the range configured for connection establishment at the backend servers. Minimum value: 1024 Maximum value: 65535

natRule When Natrule is configured and netprofile is bound to lb vserver, Citrix ADC will use the prefix of rewrite IP for outgoing packets if prefix of source IP of incoming packet matches with prefix of IP of natrule. This will take preference over USIP and USNIP configuration. ip_addr : IP for which prefix need to rewritten. netmask : Netmask for NatRule IP and RewriteIP. rewriteIp : Prefix for modified IP.

netmask rewriteIp

Example

bind netprofile npf_1 -srcportrange 2000-3000 bind netprofile npf_1 -natRule 10.0.0.0 255.0.0.0 11.0.0.0

set netProfile

Modifies the srcIP parameter of a net profile.

Synopsis

set netProfile <name>

Arguments

name Name of the net profile whose parameter you want to modify.

srcIP IP address or the name of an IP set.

srcippersistency When the net profile is associated with a virtual server or its bound services, this option enables the Citrix ADC to use the same address, specified in the net profile, to communicate to servers for all sessions initiated from a particular client to the virtual server.

Possible values: ENABLED, DISABLED Default value: DISABLED

overrideLsn USNIP/USIP settings override LSN settings for configured service/virtual server traffic..

Possible values: ENABLED, DISABLED Default value: DISABLED

MBF Response will be sent using learnt info if enabled. When creating a netprofile, if you do not set this parameter, the netprofile inherits the global MBF setting (available in the enable ns mode and disable ns mode CLI commands, or in the System > Settings > Configure modes > Configure Modes dialog box). However, you can override this setting after you create the netprofile

Possible values: ENABLED, DISABLED

proxyProtocol Proxy Protocol Action (Enabled/Disabled)

Possible values: ENABLED, DISABLED Default value: DISABLED

proxyProtocoltxversion Proxy Protocol Version (V1/V2)

Possible values: V1, V2 Default value: V1

proxyProtocolAfterTLSHandshake ADC doesnt look for proxy header before TLS handshake, if enabled. Proxy protocol parsed after TLS handshake

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set netProfile prof_1 -srcIP 10.102.1.10

add netProfile

Creates a net profile. A net profile (or network profile) contains an IP address or an IP set. During communication with physical servers or peers, the Citrix ADC uses the addresses specified in the profile as the source IP address.

Synopsis

add netProfile <name> [-proxyProtocol (ENABLED | DISABLED)]

Arguments

name Name for the net profile. Must begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the profile is created. Choose a name that helps identify the net profile.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

srcIP IP address or the name of an IP set.

srcippersistency When the net profile is associated with a virtual server or its bound services, this option enables the Citrix ADC to use the same address, specified in the net profile, to communicate to servers for all sessions initiated from a particular client to the virtual server.

Possible values: ENABLED, DISABLED Default value: DISABLED

overrideLsn USNIP/USIP settings override LSN settings for configured service/virtual server traffic..

Possible values: ENABLED, DISABLED Default value: DISABLED

MBF Response will be sent using learnt info if enabled. When creating a netprofile, if you do not set this parameter, the netprofile inherits the global MBF setting (available in the enable ns mode and disable ns mode CLI commands, or in the System > Settings > Configure modes > Configure Modes dialog box). However, you can override this setting after you create the netprofile

Possible values: ENABLED, DISABLED

proxyProtocol Proxy Protocol Action (Enabled/Disabled)

Possible values: ENABLED, DISABLED Default value: DISABLED

proxyProtocoltxversion Proxy Protocol Version (V1/V2)

Possible values: V1, V2 Default value: V1

proxyProtocolAfterTLSHandshake ADC doesnt look for proxy header before TLS handshake, if enabled. Proxy protocol parsed after TLS handshake

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

add netProfile prof1 -srcip 10.102.1.10

rm netProfile

Removes a net profile from the Citrix ADC.

Synopsis

rm netProfile <name> ...

Arguments

name Name of the net profile to be removed.

Example

rm netProfile prof1

show netProfile

Displays the settings of all net profiles configured on the Citrix ADC, or of the specified net profile.

Synopsis

show netProfile

Arguments

name Name of the net profile whose details you want to display.

Output

srcIP Source IPaddress or IPSET name.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

srcippersistency When the net profile is associated with a virtual server or its bound services, this option enables the Citrix ADC to use the same address, specified in the net profile, to communicate to servers for all sessions initiated from a particular client to the virtual server.

netprofRefcount Used to keep reference count of IP

overrideLsn USNIP/USIP settings override LSN settings for configured service/virtual server traffic..

srcPortRange When the source port range is configured and associated with the netprofile bound to a service group, Citrix ADC will choose a port from the range configured for connection establishment at the backend servers.

stateflag state flag

flags natRule IPv4 network address on whose traffic you want the Citrix ADC to do rewrite ip prefix.

netmask rewriteIp MBF Response will be sent using learnt info if enabled. When creating a netprofile, if you do not set this parameter, the netprofile inherits the global MBF setting (available in the enable ns mode and disable ns mode CLI commands, or in the System > Settings > Configure modes > Configure Modes dialog box). However, you can override this setting after you create the netprofile

proxyProtocol Proxy Protocol Action (Enabled/Disabled)

proxyProtocoltxversion Proxy Protocol Version (V1/V2)

proxyProtocolAfterTLSHandshake ADC doesnt look for proxy header before TLS handshake, if enabled. Proxy protocol parsed after TLS handshake

proxyProtocolTLVOptions Proxy protocol TLV options

devno count

Example

show netProfile

netbridge

The following operations can be performed on "netbridge":

bind| unbind| add| show| unset| set| rm|

bind netbridge

Bind a network bridge to its attributes.

Synopsis

bind netbridge <name> [-IPAddress <ip_addr|ipv6_addr|*>]

Arguments

name The name of the network bridge.

tunnel The name of the tunnel that needs to be a part of this network bridge.

vlan The VLAN that needs to be extended. Minimum value: 1 Maximum value: 4094

IPAddress The subnet that needs to be extended.

netmask Subnet mask in dotted-decimal format. For example: 255.255.255.0. This parameter is required for IPv4.

Example

bind netbridge bridge1 -tunnel tun0

unbind netbridge

Unbind a network bridge from its attributes.

Synopsis

unbind netbridge <name> [-IPAddress <ip_addr|ipv6_addr|*>]

Arguments

name The name of the network bridge.

tunnel The name of the tunnel that is part of this network bridge.

vlan The vlan that is part of this network bridge. Minimum value: 1 Maximum value: 4094

IPAddress The subnet that is part of this network bridge.

netmask Subnet mask in dotted-decimal format. For example: 255.255.255.0. This parameter is required for IPv4.

Example

unbind netbridge bridge1 -tunnel tun0

add netbridge

Add a network bridge.

Synopsis

add netbridge <name>

Arguments

name The name of the network bridge.

vxlanVlanMap The vlan to vxlan mapping to be applied to this netbridge.

Example

add netbridge bridge1

show netbridge

Show configured network bridges.

Synopsis

show netbridge

Arguments

name The name of the network bridge.

Output

vxlanVlanMap The vlan to vxlan mapping to be applied to this netbridge.

tunnel The name of the tunnel that is a part of this bridge.

vlan The VLAN that is extended by this network bridge.

IPAddress The subnet that is extended by this network bridge.

netmask The network mask for the subnet.

stateflag Used internally for display.

devno count

unset netbridge

Use this command to remove netbridge settings.Refer to the set netbridge command for meanings of the arguments.

Synopsis

unset netbridge <name> -vxlanVlanMap

set netbridge

Set network bridge parameters.

Synopsis

set netbridge <name>

Arguments

name The name of the network bridge.

vxlanVlanMap The vlan to vxlan mapping to be applied to this netbridge.

Example

set netbridge bridge1 -vlanVxlanMap p1

rm netbridge

Remove a network bridge.

Synopsis

rm netbridge <name>

Arguments

name The name of the network bridge.

Example

remove netbridge bridge1

Network

The entities on which you can perform NetScaler CLI operations:

- L2Param
- L3Param
- L4Param
- MapBmr
- MapDmr
- MapDomain
- appAlgParam
- arp
- arpparam
- bridge
- bridgegroup
- bridgetable
- channel
- ci
- fis
- forwardingSession
- inat
- inatparam
- inatsession
- interface
- interfacePair
- ip6Tunnel
- ip6TunnelParam
- ipTunnel
- ipTunnelParam
- ipset
- ipv6
- lacp
- linkset
- nat64

- nat64param
- nd6
- nd6RAvariables
- netProfile
- netbridge
- onLinkIPv6Prefix
- portallocation
- ptp
- rnat
- rnat6
- rnatglobal
- rnatip
- rnatparam
- rnatsession
- route
- route6
- rsskeytype
- tunnelip
- tunnelip6
- vlan
- vrID
- vrID6
- vrIDParam
- vxlan
- vxlanVlanMap

onLinkIPv6Prefix

The following operations can be performed on "onLinkIPv6Prefix":

unset| rm| set| show| add|

unset onLinkIPv6Prefix

Use this command to remove onLinkIPv6Prefix settings.Refer to the set onLinkIPv6Prefix command for meanings of the arguments.

Synopsis

unset onLinkIPv6Prefix <ipv6Prefix>

rm onLinkIPv6Prefix

remove an existing on-link global prefix.

Synopsis

rm onLinkIPv6Prefix <ipv6Prefix>

Arguments

ipv6Prefix Onlink prefixes for RA messages.

Example

rm onLinkIPv6Prefix 8000::/64

set onLinkIPv6Prefix

set on-link global prefix's configuration variables.

Synopsis

set onLinkIPv6Prefix <ipv6Prefix>

Arguments

ipv6Prefix Onlink prefixes for RA messages.

onlinkPrefix RA Prefix onlink flag.

Possible values: YES, NO Default value: YES

autonomusPrefix RA Prefix Autonomus flag.

Possible values: YES, NO Default value: YES

depricatePrefix Depricate the prefix.

Possible values: YES, NO Default value: NO

decrementPrefixLifeTimes RA Prefix Autonomus flag.

Possible values: YES, NO Default value: NO

prefixValideLifeTime Valide life time of the prefix, in seconds. Default value: 2592000 Minimum value: 0

prefixPreferredLifeTime Preferred life time of the prefix, in seconds. Default value: 604800 Minimum value: 0

Example

set onLinkIPv6Prefix 8000::/64 -prefixValideLifeTime 2592000

show onLinkIPv6Prefix

displays on-link global prefixes.

Synopsis

show onLinkIPv6Prefix

Arguments

ipv6Prefix Onlink prefixes for RA messages.

Output

onlinkPrefix RA Prefix onlink flag.

autonomusPrefix RA Prefix Autonomus flag.

depricatePrefix Depricate the prefix.

decrementPrefixLifeTimes RA Prefix Autonomus flag.

prefixValideLifeTime Valide life time of the prefix, in seconds.

prefixPreferredLifeTime Preferred life time of the prefix, in seconds.

stateflag RA Param state flags

prefixCurrValideLfT Prefix current valid life time

prefixCurrPreferredLfT Prefix current prefered life time

devno count

add onLinkIPv6Prefix

add a new on-link global prefix.

Synopsis

add onLinkIPv6Prefix <ipv6Prefix>

Arguments

ipv6Prefix Onlink prefixes for RA messages.

onlinkPrefix RA Prefix onlink flag.

Possible values: YES, NO Default value: YES

autonomusPrefix RA Prefix Autonomus flag.

Possible values: YES, NO Default value: YES

depricatePrefix Depricate the prefix.

Possible values: YES, NO Default value: NO

decrementPrefixLifeTimes RA Prefix Autonomus flag.

Possible values: YES, NO Default value: NO

prefixValideLifeTime Valide life time of the prefix, in seconds. Default value: 2592000 Minimum value: 0

prefixPreferredLifeTime Preferred life time of the prefix, in seconds. Default value: 604800 Minimum value: 0

Example

add onLinkIPv6Prefix 8000::/64

portallocation

The following operations can be performed on "portallocation":

show portallocation

Shows the port allocation for IPs based on given inputs parameters

Synopsis

show portallocation -destIP <ip_addr|ipv6_addr> -destPort <port> -protocol <positive_integer>

Arguments

srcIP IP address for which Port allocation needs to be seen. IP address can be SNIP/VIP/NSIP

destIP Destination IP address or Server IP for which Port allocation needs to be seen

destPort Destination Port or Server port configuration Minimum value: 1 Maximum value: 65535

protocol Protocol for the traffic. TCP traffic: 1, All other protocol traffic: 0 Minimum value: 0 Maximum value: 1

Output

freePorts Freeports for the desired IP address and other parameters

devno count stateflag

Example

show network portallocation -srcip 172.168.200.1 -destip 172.168.200.100 -destport 80 -protocol 1

ptp

The following operations can be performed on "ptp":

show| set|

show ptp

Displays the status of Precision Time Protocol (PTP) on the appliance.

Synopsis

show ptp

Arguments

Output

state Enables or disables Precision Time Protocol (PTP) on the appliance. If you disable PTP, make sure you enable Network Time Protocol (NTP) on the cluster.

set ptp

Specifies whether to use Precision Time Protocol (PTP) to synchronize time across cluster nodes. This command is applicable in a cluster setup only. If you do not want to use PTP, you must disable PTP, by using this command, and instead enable NTP.

Synopsis

set ptp -state (DISABLE | ENABLE)

Arguments

state Enables or disables Precision Time Protocol (PTP) on the appliance. If you disable PTP, make sure you enable Network Time Protocol (NTP) on the cluster.

Possible values: DISABLE, ENABLE Default value: ENABLE

rnat

The following operations can be performed on "rnat":

clear| bind| rename| unset| show| rm| unbind| set| stat| add|

clear rnat

Removes an RNAT rule from the NetScaler appliance. NOTE: This command is deprecated.Command is Deprecated, Please use "rm rnat " command to remove the RNAT rule

Synopsis

Arguments

network The network address defined for the RNAT entry.

netmask The subnet mask for the network address.

aclname An extended ACL defined for the RNAT entry.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

ownerGroup The owner node group in a Cluster for this rnat rule. Default value: DEFAULT_NG

bind rnat

Binds specified IPv4 NAT IPs to an RNAT rule.

Synopsis

bind rnat <name> (<natIP>@ ... | -retainsourceportrange <int> ...)

Arguments

name Name of the RNAT rule to which to bind NAT IPs.

natIP One or more NATIP addresses to be bound to the RNAT rule.

retainsourceportrange When the source port range is configured and associated with the RNAT rule, Citrix ADC will choose a port from the specified source port range configured for connection establishment at the backend servers. Minimum value: 1024 Maximum value: 65535

Example

bind rnat rnat1 1.1.1. 2.2.2.1 bind rnat rnat1 -retainsrcportrange 2000-3000 4024

rename rnat

Renames an RNAT rule.

Synopsis

rename rnat <name> <newName>

Arguments

name Name of the RNAT rule that you want to rename.

newName New name for the RNAT4 rule. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

Example

rename rnat rnat-rule rnat-rule-new

unset rnat

Resets the specified parameters of an RNAT rule to their default settings. Refer to the set rnat command for parameter descriptions..Refer to the set rnat command for meanings of the arguments.

Synopsis

unset rnat

show rnat

Display the Reverse NAT configuration.

Synopsis

show rnat

Arguments

name Name of the RNAT rule whose details you want to display.

Output

network The network address.

netmask Subnet mask associated with the network address.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

natIP Nat IP Address.

aclname Name of any configured extended ACL whose action is ALLOW. The condition specified in the extended ACL rule isused as the condition for the RNAT rule.

redirectPort Port number to which the IPv4 packets are redirected. Applicable to TCP and UDP protocols.

srcippersistency Enables the Citrix ADC to use the same NAT IP address for all RNAT sessions initiated from a particular server.

useproxyport Enable source port proxying, which enables the Citrix ADC to use the RNAT ips using proxied source port.

cfgflags This contains the flags for RNAT in DB

ownerGroup The owner node group in a Cluster for this rnat rule.

connfailover Synchronize all connection-related information for the RNAT sessions with the secondary ADC in a high availability (HA) pair.

retainsourceportrange When the source port range is configured and associated with the RNAT rule, Citrix ADC will choose a port from the specified source port range configured for connection establishment at the backend servers.

stateflag devno count

rm rnat

Remove the specified RNAT rule.

Synopsis

rm rnat <name>@ ...

Arguments

name Name of the RNAT rule entry to be removed from the NetScaler appliance.

Example

rm rnat rnat_rule

unbind rnat

Unbinds the associated NAT IP4 address(es) from an RNAT rule.

Synopsis

unbind rnat <name> (<natIP>@ ... | -retainsourceportrange <int> ...)

Arguments

name Name of the RNAT rule from which to unbind the associated NAT IP address(es).

natIP IP address, or multiple NATIP addresses, to be unbound from the RNATrule. (If using the CLI, use spaces to separate multiple addresses.)

retainsourceportrange When the source port range is configured and associated with the RNAT rule, Citrix ADC will choose a port from the specified source port range configured for connection establishment at the backend servers. Minimum value: 1024 Maximum value: 65535

Example

unbind rnat rnat1 1.1.1. 2.2.2.1 unbind rnat rnat1 -retainsrcportrange 2000-3000 4024

set rnat

Modifies parameters of an RNAT rule.

Synopsis

set rnat

Arguments

name Name for the RNAT4 rule. Must begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the rule is created. Choose a name that helps identify the RNAT4 rule.

redirectPort Port number to which the IPv4 packets are redirected. Applicable to TCP and UDP protocols. Minimum value: 1 Maximum value: 65535

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

srcippersistency Enables the Citrix ADC to use the same NAT IP address for all RNAT sessions initiated from a particular server.

Possible values: ENABLED, DISABLED Default value: DISABLED

useproxyport Enable source port proxying, which enables the Citrix ADC to use the RNAT ips using proxied source port.

Possible values: ENABLED, DISABLED Default value: ENABLED

ownerGroup The owner node group in a Cluster for this rnat rule. Default value: DEFAULT_NG

connfailover Synchronize all connection-related information for the RNAT sessions with the secondary ADC in a high availability (HA) pair.

Possible values: ENABLED, DISABLED Default value: DISABLED

stat rnat

Display statistics for rnat sessions.

Synopsis

stat rnat

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Bytes Received (rnatRxBytes) Bytes received during RNAT sessions.

Bytes Sent (rnatTxBytes) Bytes sent during RNAT sessions.

Packets Received (rnatRxPkts) Packets received during RNAT sessions.

Packets Sent (rnatTxPkts) Packets sent during RNAT sessions.

Syn Sent (rnatTxSyn) Requests for connections sent during RNAT sessions.

Current RNAT sessions (rnatSessions) Currently active RNAT sessions.

Example

stat rnat

Related Commands

- stat MapDomain

add rnat

Adds a Reverse Network Address Translation (RNAT) rule for IPv4 traffic. When an IPv4 packet generated by a servermatches the conditions specified in the RNAT rule, the appliance replaces

the source IPv4 address of the IPv4 packet with a configured NAT IPv4 address before forwarding it to the destination.

Synopsis

add rnat <name> ((<network>) | (<aclname>))

Arguments

name Name for the RNAT4 rule. Must begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the rule is created. Choose a name that helps identify the RNAT4 rule.

network IPv4 network address on whose traffic you want the Citrix ADC to do RNAT processing.

netmask Subnet mask associated with the network address.

aclname Name of any configured extended ACL whose action is ALLOW. The condition specified in the extended ACL rule isused as the condition for the RNAT rule.

redirectPort Port number to which the IPv4 packets are redirected. Applicable to TCP and UDP protocols. Minimum value: 1 Maximum value: 65535

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

srcippersistency Enable source ip persistency, which enables the NetScaler appliance to use the RNAT ips using source ip.

Possible values: ENABLED, DISABLED Default value: DISABLED

useproxyport Enable source port proxying, which enables the NetScaler appliance to use the RNAT ips using proxied source port.

Possible values: ENABLED, DISABLED Default value: ENABLED

connfailover Synchronize all connection-related information for the RNAT sessions with the secondary ADC in a high availability (HA) pair.

Possible values: ENABLED, DISABLED Default value: DISABLED

ownerGroup The owner node group in a Cluster for this rnat rule. Default value: DEFAULT_NG

Example

add rnat rnat1 192.168.10.0 255.255.255.0 or add rnat rnat1 acl1

rnat6

The following operations can be performed on "rnat6":

stat| clear| set| unbind| show| bind| unset| add|

stat rnat6

Display statistics for rnat6 sessions.

Synopsis

stat rnat6

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Bytes Received (rnat6RxBytes) Bytes received during RNAT6 sessions.

Bytes Sent (rnat6TxBytes) Bytes sent during RNAT6 sessions.

Packets Received (rnat6RxPkts) Packets received during RNAT6 sessions.

Packets Sent (rnat6TxPkts) Packets sent during RNAT6 sessions.

Syn Sent (rnat6TxSyn) Requests for connections sent during RNAT6 sessions.

Current RNAT6 sessions (rnat6Sessions) Currently active RNAT6 sessions.

Example

stat rnat6

Related Commands

- stat MapDomain

clear rnat6

Removes an RNAT6 rule from the Citrix ADC.

Synopsis

clear rnat6 <name>

Arguments

name Name of the RNAT6 rule to be removed.

ownerGroup The owner node group in a Cluster for this rnat rule. Default value: DEFAULT_NG

set rnat6

Modifies the specified parameters of an RNAT6 rule.

Synopsis

set rnat6 <name>

Arguments

name Name of the RNAT6 rule. Required for identifying the RNAT6 rule and cannot be modified.

redirectPort Port number to which the IPv6 packets are redirected. Applicable to TCP and UDP protocols. Minimum value: 1 Maximum value: 65535

srcippersistency Enable source ip persistency, which enables the Citrix ADC to use the RNAT6 ips using source ip.

Possible values: ENABLED, DISABLED Default value: DISABLED

ownerGroup The owner node group in a Cluster for this rnat rule. Default value: DEFAULT_NG

unbind rnat6

Unbinds the associated NAT IPv6 address(es) from an RNAT6 rule.

Synopsis

unbind rnat6 <name> <natIP6>@ ...

Arguments

name Name of the RNAT6 rule from which to unbind the associated NAT IP address(es).

natIP6 IP address, or multiple addresses, to be unbound from the RNAT6rule. (If using the CLI, use spaces to separate multiple addresses.)

Example

unbind rnat6 <rnat6_name> <natIP6>@ ...

show rnat6

Displays the settings of all RNAT6 rules configured on the Citrix ADC, or of the specified RNAT6 rule.

Synopsis

show rnat6

Arguments

name Name of the RNAT6 rule whose details you want to display.

Output

network The network address.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

acl6name ACL6 name

natIP6 Nat IP Address.

redirectPort Redirect Port Value

srcippersistency Enable source ip persistency, which enables the Citrix ADC to use the RNAT6 ips using source ip.

ownerGroup The owner node group in a Cluster for this rnat rule.

stateflag devno count

bind rnat6

Binds specified IPv6 NAT IPs to an RNAT6 rule.

Synopsis

bind rnat6 <name> <natIP6>@ ...

Arguments

name Name of the RNAT6 rule to which to bind NAT IPs.

natIP6 One or more IP addresses to be bound to the IP set.

Example

bind rnat6 <rnat6_name> <natIP6>@ ...

unset rnat6

Resets the specified parameters of an RNAT6 rule to their default settings. Refer to the set rnat6 command for parameter descriptions..Refer to the set rnat6 command for meanings of the arguments.

Synopsis

unset rnat6 <name>

add rnat6

Adds a Reverse Network Address Translation (RNAT6) rule for IPv6 traffic. When an IPv6 packet generated by a server matches the conditions specified in the RNAT6 rule, the appliance replaces the source IPv6 address of the IPv6 packet with a configured NAT IPv6 address before forwarding it to the destination.

Synopsis

add rnat6 <name> (<network> | (<acl6name>))

Arguments

name Name for the RNAT6 rule. Must begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the rule is created. Choose a name that helps identify the RNAT6 rule.

network IPv6 address of the network on whose traffic you want the Citrix ADC to do RNAT processing.

acl6name Name of any configured ACL6 whose action is ALLOW. The rule of the ACL6 is used as an RNAT6 rule.

redirectPort Port number to which the IPv6 packets are redirected. Applicable to TCP and UDP protocols. Minimum value: 1 Maximum value: 65535

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

srcippersistency Enable source ip persistency, which enables the Citrix ADC to use the RNAT ips using source ip.

Possible values: ENABLED, DISABLED Default value: DISABLED

ownerGroup The owner node group in a Cluster for this rnat rule. Default value: DEFAULT_NG

Example

add rnat6 rnat6_name 2002::/64

rnatglobal

The following operations can be performed on "rnatglobal":

unbind| bind| show|

unbind rnatglobal

Unbind policy from rnat

Synopsis

unbind rnatglobal (-policy <string> | -all)

Arguments

policy Name of the policy to be unbound from the RNAT globally.

all Remove all RNAT global config

bind rnatglobal

Bind rnat to policy for logging purpose

Synopsis

bind rnatglobal [-policy <string>]

Arguments

policy Name of the policy getting bound to the RNAT globally. This policy will apply to all the RNATS present

priority Priority of the policy Minimum value: 0

show rnatglobal

Display the Reverse NAT configuration.

Synopsis

show rnatglobal

Arguments

Output

policy The policy Name.

stateflag priority The priority of the policy.

devno count

rnatip

The following operations can be performed on "rnatip":

stat rnatip

Display statistics for RNAT sessions.

Synopsis

stat rnatip

Arguments

rnatip Specifies the NAT IP address of the configured RNAT entry for which you want to see the statistics. If you do not specify an IP address, this displays the statistics for all the configured RNAT entries.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Traffic domain (td) Traffic domain for ipaddr.

Bytes Received (rxBytes) Bytes received on this IP address during RNAT sessions.

Bytes Sent (txBytes) Bytes sent from this IP address during RNAT sessions.

Packets Received (rxPkts) Packets received on this IP address during RNAT sessions.

Packets Sent (txPkts) Packets sent from this IP address during RNAT sessions.

Syn Sent (txSyn) Requests for connections sent from this IP address during RNAT sessions.

Current RNAT sessions (sessions) Currently active RNAT sessions started from this IP address.

Example

stat rnatip 1.1.1.1

Related Commands

- stat MapDomain

rnatparam

The following operations can be performed on "rnatparam":

show| unset| set|

show rnatparam

Show the rnat parameter.

Synopsis

show rnatparam

Arguments

Output

tcpproxy Enable TCP proxy, which enables the Citrix ADC to optimize the RNAT TCP traffic by using Layer 4 features.

srcippersistency Enable source ip persistency, which enables the Citrix ADC to use the RNAT ips using source ip.

Example

show rnat parameter

unset rnatparam

Use this command to remove rnatparam settings.Refer to the set rnatparam command for meanings of the arguments.

Synopsis

unset rnatparam

set rnatparam

Sets global parameters of RNAT rules on the Citrix ADC.

Synopsis

set rnatparam

Arguments

tcpproxy Enable TCP proxy, which enables the Citrix ADC to optimize the RNAT TCP traffic by using Layer 4 features.

Possible values: ENABLED, DISABLED Default value: ENABLED

srcippersistency Enable source ip persistency, which enables the Citrix ADC to use the RNAT ips using source ip.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set rnatparam -tcpproxy ENABLED or set rnatparam -srcippersistency ENABLED.

rnatsession

The following operations can be performed on "rnatsession":

flush rnatsession

Flush RNAT Session.

Synopsis

flush rnatsession ((-network <ip_addr> -netmask <netmask>) | -natIP <ip_addr> | -aclname <string>)

Arguments

network IPv4 network address on whose traffic you want the Citrix ADC to do RNAT processing.

netmask Subnet mask associated with the network address.

natIP The NAT IP address defined for the RNAT entry.

aclname Name of any configured extended ACL whose action is ALLOW.

Example

To flush all RNAT sessions : flush rnatsession. To flush Network based RNAT sessions: flush rnatsession -network 10.10.1.0 -netmask 255.255.255.0. To flush ACL based RNAT sessions: flush rnatsession -aclname acl. To flush RNAT sessions for a specific NATIP : flush rnatsession -natip 10.101.10.1.

route

The following operations can be performed on "route":

clear| rm| set| add| show| unset|

clear route

Removes routes of the specifiedtype(protocol) from the routing table of the Citrix ADC.

Synopsis

clear route <routeType>

Arguments

routeType Protocol used by routes that you want to remove from the routing table of the Citrix ADC.

rm route

Removes a static route from the Citrix ADC. Note: You cannot use this command to remove routes that are part of a VLAN configuration. Use the rmvlan or clear vlan command instead.

Synopsis

rm route <network> <netmask> (<gateway> | -vlan <positive_integer>)

Arguments

network Network address specified in the route entry that you want to remove from the routing table of the Citrix ADC.

netmask Subnet mask associated with the network address.

gateway IP address of the gateway for this route.

vlan Gateway vlan for this route. Minimum value: 1 Maximum value: 4094

td The Traffic Domain Id of the route to be removed. Minimum value: 0 Maximum value: 4094

ownerGroup The owner node group in a Cluster for this route. If owner node group is not specified then the route is treated as Striped route. Default value: DEFAULT_NG

Related Commands

- clear vlan

set route

Modifies parameters of an IPv4 static route.

Synopsis

set route <network> <netmask> <gateway> [-msr (ENABLED | DISABLED)]

Arguments

network Network address in the route entry that you want to modify.

netmask Subnet mask associated with the network address.

gateway IP address of the gateway for this route. Can be either the IP address of the gateway, or can be null to specify a null interface route.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

distance Administrative distance of this route, which determines the preference of this route over other routes, with same destination, from different routing protocols. A lower value is preferred. Default value: 1 Minimum value: 0 Maximum value: 255

cost The cost of a route is used to compare routes of the same type. The route having the lowest cost is the most preferred route. Possible values: 0 through 65535. Default: 0. Minimum value: 0 Maximum value: 65535

weight Positive integer used by the routing algorithms to determine preference for this route over others of equal cost. The lower the weight, the higher the preference. Default value: 1 Minimum value: 1 Maximum value: 65535

advertise Advertise this route.

Possible values: DISABLED, ENABLED

protocol Routing protocol used for advertising this route. Default value: ADV_ROUTE_FLAGS

msr Monitor this route using a monitor of type ARP or PING.

Possible values: ENABLED, DISABLED Default value: DISABLED

monitor Name of the monitor, of type ARP or PING, configured on the Citrix ADC to monitor this route.

Example

set route 10.10.10.0 255.255.255.0 10.10.10.1 -advertise enable

add route

Adds an IPv4 static route to the routing table of the Citrix ADC.

Synopsis

add route <network> <netmask> (<gateway> | -vlan <positive_integer>) [-msr (ENABLED | DISABLED)]

Arguments

network IPv4 network address for which to add a route entry in the routing table of the Citrix ADC.

netmask The subnet mask associated with the network address.

gateway IP address of the gateway for this route. Can be either the IP address of the gateway, or can be null to specify a null interface route.

vlan VLAN as the gateway for this route. Minimum value: 1 Maximum value: 4094

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

distance Administrative distance of this route, which determines the preference of this route over other routes, with same destination, from different routing protocols. A lower value is preferred. Default value: 1 Minimum value: 0 Maximum value: 255

cost The cost of a route is used to compare routes of the same type. The route having the lowest cost is the most preferred route. Possible values: 0 through 65535. Default: 0. Minimum value: 0 Maximum value: 65535

weight Positive integer used by the routing algorithms to determine preference for this route over others of equal cost. The lower the weight, the higher the preference. Default value: 1 Minimum value: 1 Maximum value: 65535

advertise Advertise this route.

Possible values: DISABLED, ENABLED

protocol Routing protocol used for advertising this route. Default value: ADV_ROUTE_FLAGS

msr Monitor this route using a monitor of type ARP or PING.

Possible values: ENABLED, DISABLED Default value: DISABLED

monitor Name of the monitor, of type ARP or PING, configured on the Citrix ADC to monitor this route.

ownerGroup The owner node group in a Cluster for this route. If owner node group is not specified then the route is treated as Striped route. Default value: DEFAULT_NG

Example

add route 10.10.10.0 255.255.255.0 10.10.10.1

Related Commands

- rm arp

show route

Display the configured routing information.

Synopsis

show route [<network> <netmask>]

Arguments

network The destination network or host.

netmask The subnet mask associated with the network address.

gateway The gateway for the route.

vlan The gateway vlan for the route. Minimum value: 1 Maximum value: 4094

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

routeType The type of routes to be shown.

detail Display a detailed view.

Output

gatewayName The name of the gateway for this route. For a route other than a link load balancing (LLB) route, this value is null.

advertise Enable advertisement.

type State of the RNAT.

stateflag dynamic State of the route.

STATIC PERMANENT DIRECT NAT LBROUTE ADV TUNNEL Show whether it is a tunnel route or not.

cost Cost of this route.

distance Administrative distance of this route, which determines the preference of this route over other routes, with same destination, from different routing protocols. A lower value is preferred.

cost The cost of a route is used to compare routes of the same type. The route having the lowest cost is the most preferred route. Possible values: 0 through 65535. Default: 0.

weight The weight of this route.

protocol Routing protocol used for advertising this route.

data Internal data of this route.

data0 Internal route type is stored, used for get.

flags If this route is dynamic, the name of the routing protocol from which it was learned.

routeOwners Use this option with -dynamic and in a cluster only to specify the set of nodes from which this dynamic route has been learnt.

retain OSPF OSPF protocol.

ISIS ISIS protocol.

RIP RIP protocol.

BGP BGP protocol.

DHCP advOSPF Advertised through OSPF protocol.

advISIS Advertised through ISIS protocol.

advRIP Advertised through RIP protocol.

advBGP Advertised through BGP protocol.

msr Whether MSR is enabled or disabled.

monitor Name of the monitor, of type ARP or PING, configured on the Citrix ADC to monitor this route.

state The state of the static route. Possible values: UP, DOWN.

peFlags PE flags.

totalprobes The total number of probes sent.

totalfailedprobes The total number of failed probes.

failedprobes Number of the current failed monitoring probes.

monStatCode The code indicating the monitor response.

monStatParam1 First parameter used with the message code.

monStatParam2 Second parameter used with the message code.

monStatParam3 Third parameter used with the message code.

ownerGroup The owner node group in a Cluster for this route. If owner node group is not specified then the route is treated as Striped route.

clusterFlags Flags for cluster. Currently used to determine if it is a cluster system

devno count

Example

An example of the output of the show route command is as follows:

3 configured routes:

```
Network        Netmask        Gateway/OwnedIP     Type

-------        -------        ---------------     ----
```

1. 0.0.0.0 0.0.0.0 10.11.0.254 STATIC
2. 127.0.0.0 255.0.0.0 127.0.0.1 PERMANENT
3. 10.251.0.0 255.255.0.0 10.251.0.254 NAT

unset route

Unset the attributes of a route that were added by the add/set route command..Refer to the set route command for meanings of the arguments.

Synopsis

unset route <network> <netmask> <gateway>

Example

unset route 10.10.10.0 255.255.255.0 10.10.10.1 -advertise enable

route6

The following operations can be performed on "route6":

rm| set| unset| clear| show| add|

rm route6

Removes a static IPv6 route from the Citrix ADC.

Synopsis

rm route6 <network>

Arguments

network The network of the route to be removed.

gateway The gateway address of the route to be removed. Default value: 0

vlan Integer that uniquely identifies the VLAN defined for this route. Default value: 0 Minimum value: 0 Maximum value: 4094

vxlan Integer value that uniquely identifies a VXLAN through which the Citrix ADC forwards the packets for this route. Minimum value: 1 Maximum value: 16777215

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

ownerGroup The owner node group in a Cluster for this route6. If owner node group is not specified then the route is treated as Striped route. Default value: DEFAULT_NG

Example

rm route6 ::/0 2004::1 rm route6 ::/0 FE80::67 -vlan 5

set route6

Modifies parameters of an IPv6 static route.

Synopsis

set route6 <network> [-msr (ENABLED | DISABLED)]

Arguments

network IPv6 network address of the route entry to be modified.

gateway The gateway for the route's destination network. Default value: 0

vlan Integer value that uniquely identifies a VLAN through which the Citrix ADC forwards the packets for this route. Default value: 0 Minimum value: 0 Maximum value: 4094

vxlan Integer value that uniquely identifies a VXLAN through which the Citrix ADC forwards the packets for this route. Minimum value: 1 Maximum value: 16777215

weight Positive integer used by the routing algorithms to determine preference for this route over others of equal cost. The lower the weight, the higher the preference. Default value: 1 Minimum value: 1 Maximum value: 65535

distance Administrative distance of this route from the appliance. Default value: 1 Minimum value: 1 Maximum value: 254

cost Positive integer used by the routing algorithms to determine preference for this route. The lower the cost, the higher the preference. Default value: 1 Minimum value: 0 Maximum value: 65535

advertise Advertise this route.

Possible values: DISABLED, ENABLED

msr Monitor this route with a monitor of type ND6 or PING.

Possible values: ENABLED, DISABLED Default value: DISABLED

monitor Name of the monitor, of type ND6 or PING, configured on the Citrix ADC to monitor this route.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

Example

set route6 1::1/100 2000::1 -advertise enable

unset route6

Unset the attributes of a route that were added by the add/set route command..Refer to the set route6 command for meanings of the arguments.

Synopsis

unset route6 <network>

Example

unset route6 2000::1/100 3000::1 -advertise enable

clear route6

Removes IPv6 routes of the specified type (protocol) from the routing table of the Citrix ADC.

Synopsis

clear route6 <routeType>

Arguments

routeType Type of IPv6 routes to remove from the routing table of the Citrix ADC.

show route6

Displays configuration and state information of all IPv6 routes in the Citrix ADC's routing table, or of the specified IPv6 route.

Synopsis

show route6 [<network>]

Arguments

network IPv6 network address of the route entry for which to display details.

gateway Any gateway of the route entry for which to display details. Default value: 0

vlan Integer that uniquely identifies the VLAN defined for this route. Default value: 0 Minimum value: 0 Maximum value: 4094

vxlan Integer value that uniquely identifies a VXLAN through which the Citrix ADC forwards the packets for this route. Minimum value: 1 Maximum value: 16777215

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

routeType The type of IPv6 routes to be to be displayed.

detail To get a detailed view.

Output

gatewayName The name of the gateway for this route.

advertise Any gateway of the route entry for which the details are to be displayed.

type State of the RNAT.

stateflag dynamic Whether this route is dynamically learned or not.

weight Weight of this route.

distance Administrative distance of this route from the appliance.

cost Positive integer used by the routing algorithms to determine preference for this route. The lower the cost, the higher the preference.

data Internal data of this route.

flags For a dynamic route, the routing protocol from which the route was learned.

msr Whether MSR is enabled or disabled.

monitor Name of the monitor, of type ND6 or PING, configured on the Citrix ADC to monitor this route.

state Whether this route is UP or DOWN.

totalprobes The total number of probes sent.

totalfailedprobes The total number of failed probes.

failedprobes Current number of failed monitoring probes.

monStatCode The code indicating the monitor response.

monStatParam1 First parameter for use with message code.

monStatParam2 Second parameter for use with message code.

monStatParam3 Third parameter for use with message code.

data1 Internal data of this route.

routeOwners Use this option with -dynamic and in a cluster only to specify the set of nodes from which this dynamic route has been learnt.

retain STATIC Static route.

PERMANENT Permanent Route.

connected Connected Route.

OSPFV3 For a dynamic route, the routing protocol from which the route was learned.

ISIS If this route is dynamic then which routing protocol was it learnt from.

active For a dynamic route, the routing protocol from which the route was learned.

BGP For a dynamic route, the routing protocol from which the route was learned.

RIP For a dynamic route, the routing protocol from which the route was learned.

raRoute For a dynamic route, the routing protocol from which the route was learned.

ownerGroup The owner node group in a Cluster for this route6. If owner node group is not specified then the route is treated as Striped route.

clusterFlags Flags for cluster. Currently used to determine if it is a cluster system

devno count

Example

Following is an example of the output of the show route6 command:

```
Flags: Static(S), Dynamic(D), Active(A)

---------------------------------------



Network       Gateway(vlan)   Flags

-------       -----------     -----

0::0/0        2001::1            S(A)

0::0/0        FE80::90(4)        D(A)
```

add route6

Adds an IPv6 static route to the routing table of the Citrix ADC.

Synopsis

add route6 <network> [-msr (ENABLED | DISABLED)]

Arguments

network IPv6 network address for which to add a route entry to the routing table of the Citrix ADC.

gateway The gateway for this route. The value for this parameter is either an IPv6 address or null. Default value: 0

vlan Integer value that uniquely identifies a VLAN through which the Citrix ADC forwards the packets for this route. Default value: 0 Minimum value: 0 Maximum value: 4094

vxlan Integer value that uniquely identifies a VXLAN through which the Citrix ADC forwards the packets for this route. Minimum value: 1 Maximum value: 16777215

weight Positive integer used by the routing algorithms to determine preference for this route over others of equal cost. The lower the weight, the higher the preference. Default value: 1 Minimum value: 1 Maximum value: 65535

distance Administrative distance of this route from the appliance. Default value: 1 Minimum value: 1 Maximum value: 254

cost Positive integer used by the routing algorithms to determine preference for this route. The lower the cost, the higher the preference. Default value: 1 Minimum value: 0 Maximum value: 65535

advertise Advertise this route.

Possible values: DISABLED, ENABLED

msr Monitor this route with a monitor of type ND6 or PING.

Possible values: ENABLED, DISABLED Default value: DISABLED

monitor Name of the monitor, of type ND6 or PING, configured on the Citrix ADC to monitor this route.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

ownerGroup The owner node group in a Cluster for this route6. If owner node group is not specified then the route is treated as Striped route. Default value: DEFAULT_NG

Example

add route6 ::/0 2004::1 add route6 ::/0 FE80::67 -vlan 5

rsskeytype

The following operations can be performed on "rsskeytype":

set| show|

set rsskeytype

Synopsis

set rsskeytype -rsstype (ASYMMETRIC | SYMMETRIC)

Arguments

rsstype Type of RSS key, possible values are SYMMETRIC and ASYMMETRIC.

Possible values: ASYMMETRIC, SYMMETRIC Default value: ASYMMETRIC

show rsskeytype

Synopsis

show rsskeytype

Arguments

Output

rsstype Type of RSS key, possible values are SYMMETRIC and ASYMMETRIC.

tunnelip

The following operations can be performed on "tunnelip":

stat tunnelip

Display the statistics related to IP tunnel.

Synopsis

stat tunnelip

Arguments

tunnelip remote IP address of the configured tunnel.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Packets received on tunnel (tnlRxPkts) Total number of packets received on the tunnel.

Packets transmitted on tunnel (tnlTxPkts) Total number of packets transmitted on the tunnel.

Bytes received on tunnel (tnlRxBytes) Total number of bytes received on the tunnel.

Bytes transmitted on tunnel (tnlTxBytes) Total number of bytes transmitted on the tunnel.

Example

stat tunnelip 2.1.1.1

Related Commands

- stat MapDomain

tunnelip6

The following operations can be performed on "tunnelip6":

stat tunnelip6

Display the statistics related to IP tunnel.

Synopsis

stat tunnelip6

Arguments

tunnelip6 remote IPv6 address of the configured tunnel.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Packets received on tunnel (tnlRxPkts) Total number of packets received on the tunnel.

Packets transmitted on tunnel (tnlTxPkts) Total number of packets transmitted on the tunnel.

Bytes received on tunnel (tnlRxBytes) Total number of bytes received on the tunnel.

Bytes transmitted on tunnel (tnlTxBytes) Total number of bytes transmitted on the tunnel.

Example

stat tunnelip6 2001::1

Related Commands

- stat MapDomain

vlan

The following operations can be performed on "vlan":

unbind| show| stat| add| bind| rm| set| unset|

unbind vlan

Unbinds the specified interfaces or IP addresses from a VLAN. If any of the interfaces are untagged members of the VLAN, they are automatically bound to VLAN 1.

Synopsis

unbind vlan <id> [-ifnum <interface_name> ...] [-IPAddress <ip_addr|ipv6_addr|*>]

Arguments

id The virtual LAN (VLAN) id. Minimum value: 1 Maximum value: 4094

ifnum Interface to unbind from the VLAN, specified in slot/port notation (for example, 1/3). Minimum value: 1

tagged The 802.1q tagged interface.

IPAddress The IP Address associated with the VLAN configuration.

netmask Subnet mask for the network address defined for this VLAN.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

ownerGroup The owner node group in a Cluster for this vlan. Default value: DEFAULT_NG

show vlan

Displays the settings of all VLANs configured on the Citrix ADC, or of the specified VLAN. To display the settings of all the VLANs, run the command without any parameters. To display the settings of a particular VLAN, specify the ID of the VLAN.

Synopsis

show vlan show vlan stats - alias for 'stat vlan'

Arguments

id Integer that uniquely identifies the VLAN for which the details are to be displayed. Minimum value: 1 Maximum value: 4094

Output

aliasName A name for the VLAN. Must begin with a letter, a number, or the underscore symbol, and can consist of from 1 to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the VLAN. However, you cannot perform any VLAN operation by specifying this name instead of the VLAN ID.

IPAddress The IP address assigned to the VLAN.

netmask Subnet mask for the network address defined for this VLAN.

linklocalIPv6Addr The link-local IP address assigned to the VLAN.

rnat Temporary flag used for internal purpose.

stateflag state flag

portbitmap Member interfaces of this vlan.

lsbitmap Member linksets of this vlan.

tagbitmap Tagged members of this vlan.

lstagbitmap Tagged linksets of this vlan.

ifaces Names of all member interfaces of this vlan.

tagIfaces Names of all tagged member interfaces of this vlan.

dynamicRouting Whether dynamic routing is enabled or disabled.

ipv6DynamicRouting Whether ipv6 dynamic routing is enabled or disabled.

flag ifnum The interface to be bound to the VLAN, specified in slot/port notation (for example, 1/3).

tagged Make the interface an 802.1q tagged interface. Packets sent on this interface on this VLAN have an additional 4-byte 802.1q tag, which identifies the VLAN. To use 802.1q tagging, you must also configure the switch connected to the appliance's interfaces.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

vlantd Traffic domain associated with vlan.

sdxVlan SDX vlan.

mtu Specifies the maximum transmission unit (MTU), in bytes. The MTU is the largest packet size, excluding 14 bytes of ethernet header and 4 bytes of crc, that can be transmitted and received over this VLAN.

sharing If sharing is enabled, then this vlan can be shared across multiple partitions by binding it to all those partitions. If sharing is disabled, then this vlan can be bound to only one of the partitions.

partitionName Name of the Partition to which this vlan bound to.

vxlan The VXLAN that extends this vlan.

ownerGroup The owner node group in a Cluster for this vlan.

devno count

Example

An example of the output of the show vlan command is as follows:

```
1.  VLAN ID: 5      VLAN Alias Name:

    Interfaces : 1/7

    IPs :
```

10.102.169.36 Mask: 255.255.255.0

```
1.  VLAN ID: 3      VLAN Alias Name:

    Interfaces : 1/5(T)

    Channels : LA/2 LR/1
```

Done

*(T) - Tagged

stat vlan

Display statistics for VLAN(s).

Synopsis

stat vlan

Arguments

id An integer specifying the VLAN identification number (VID). Possible values: 1 through 4094. Minimum value: 1 Maximum value: 4094

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Packets received (RxPkts) Packets received on the VLAN.

Bytes received (RxBytes) Bytes of data received on the VLAN.

Packets sent (TxPkts) Packets transmitted on the VLAN.

Bytes sent (TxBytes) Bytes of data transmitted on the VLAN.

Packets dropped (DropPkts) Inbound packets dropped by the VLAN upon reception.

Broadcast pkts sent & received (BcastPkt) Broadcast packets sent and received on the VLAN.

Example

stat vlan 1

Related Commands

- stat MapDomain

add vlan

Adds a VLAN to the Citrix ADC.The newVLAN is not active unless interfaces are bound to it.

Synopsis

add vlan <id>

Arguments

id A positive integer that uniquely identifies a VLAN. Minimum value: 1 Maximum value: 4094

aliasName A name for the VLAN. Must begin with a letter, a number, or the underscore symbol, and can consist of from 1 to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the VLAN. However, you cannot perform any VLAN operation by specifying this name instead of the VLAN ID.

dynamicRouting Enable dynamic routing on this VLAN.

Possible values: ENABLED, DISABLED Default value: DISABLED

ipv6DynamicRouting Enable all IPv6 dynamic routing protocols on this VLAN. Note: For the ENABLED setting to work, you must configure IPv6 dynamic routing protocols from the VTYSH command line.

Possible values: ENABLED, DISABLED Default value: DISABLED

mtu Specifies the maximum transmission unit (MTU), in bytes. The MTU is the largest packet size, excluding 14 bytes of ethernet header and 4 bytes of crc, that can be transmitted and received over this VLAN. Default value: 0 Minimum value: 500 Maximum value: 9216

sharing If sharing is enabled, then this vlan can be shared across multiple partitions by binding it to all those partitions. If sharing is disabled, then this vlan can be bound to only one of the partitions.

Possible values: ENABLED, DISABLED Default value: DISABLED

bind vlan

Binds the specified interfaces or IP addresses to a VLAN. An interface can be bound to a VLAN as a tagged or an untagged member. Adding an interface as an untagged member removes it from its current native VLAN and adds it to the new VLAN. If an interface is added as a tagged member to a VLAN, it still remains a member of its native VLAN.

Synopsis

bind vlan <id> [-ifnum <interface_name> ...] [-IPAddress <ip_addr|ipv6_addr|*>]

Arguments

id Specifies the virtual LAN ID. Minimum value: 1 Maximum value: 4094

ifnum Interface to be bound to the VLAN, specified in slot/port notation (for example, 1/3). Minimum value: 1

tagged Make the interface an 802.1q tagged interface. Packets leaving this interface have an additional 4-byte 802.1q tag, which identifies the VLAN. To use 802.1q tagging, you must also configure the switch connected to the interfaces on the appliance.

IPAddress Network address to be associated with the VLAN. Should exist on the appliance before you associate it with the VLAN. To enable IP forwarding among VLANs, the specified address can be used as the default gateway by the hosts in the network.

netmask Subnet mask for the network address defined for this VLAN.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

ownerGroup The owner node group in a Cluster for this vlan. Default value: DEFAULT_NG

rm vlan

Removes a VLAN from the Citrix ADC. When the VLAN is removed, its interfaces are bound to VLAN 1. Note: VLAN 1 cannot be removed by any command.

Synopsis

rm vlan <id>

Arguments

id Integer that uniquely identifies the VLAN to be removed from the Citrix ADC. When the VLAN is removed, its interfaces become members of VLAN 1. Minimum value: 2 Maximum value: 4094

set vlan

Modifies parameters of a VLAN on the Citrix ADC.

Synopsis

set vlan <id>

Arguments

id A positive integer that uniquely identifies a VLAN. Minimum value: 1 Maximum value: 4094

aliasName A name for the VLAN. Must begin with a letter, a number, or the underscore symbol, and can consist of from 1 to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the VLAN. However, you cannot perform any VLAN operation by specifying this name instead of the VLAN ID.

dynamicRouting Enable dynamic routing on this VLAN.

Possible values: ENABLED, DISABLED Default value: DISABLED

ipv6DynamicRouting Enable IPv6 dynamic routing on this vlan. Note: For the ENABLED setting to work, you must configure IPv6 dynamic routing protocols from the VTYSH command line.

Possible values: ENABLED, DISABLED Default value: DISABLED

mtu Specifies the maximum transmission unit (MTU), in bytes. The MTU is the largest packet size, excluding 14 bytes of ethernet header and 4 bytes of crc, that can be transmitted and received over this VLAN. Default value: 0 Minimum value: 500 Maximum value: 9216

sharing If sharing is enabled, then this vlan can be shared across multiple partitions by binding it to all those partitions. If sharing is disabled, then this vlan can be bound to only one of the partitions.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set vlan 2 -dynamicRouting ENABLED

unset vlan

Use this command to remove vlan settings.Refer to the set vlan command for meanings of the arguments.

Synopsis

unset vlan <id>

vrID

The following operations can be performed on "vrID":

show| bind| unset| unbind| set| rm| add|

show vrID

Displays the settings of all VRIDs configured on the Citrix ADC, or of the specified VRID. To display the settings of all the VRIDs, run the command without any parameters. To display the settings of a particular VRID, specify the VRID.

Synopsis

show vrID

Arguments

id Integer value that uniquely identifies the VMAC address. Minimum value: 1 Maximum value: 255

Output

ifaces Interfaces bound to this VRID.

ifnum Interfaces to bind to the VMAC, specified in (slot/port) notation (for example, 1/2).Use spaces to separate multiple entries.

type Indicates whether this VRID entry was added manually or dynamically. When you manually add a VRID entry, the value for this parameter is STATIC. Otherwise, it is DYNAMIC.

vlan The VLAN in which this VRID resides.

priority Base priority (BP), in an active-active mode configuration, which ordinarily determines the master VIP address.

effectivePriority The effective priority of this VRID.

preemption In an active-active mode configuration, make a backup VIP address the master if its priority becomes higher than that of a master VIP address bound to this VMAC address. If you disable pre-emption while a backup VIP address is the master, the backup VIP address remains master until the original master VIP's priority becomes higher than that of the current master.

sharing In an active-active mode configuration, enable the backup VIP address to process any traffic instead of dropping it.

tracking The effective priority (EP) value, relative to the base priority (BP) value in an active-active mode configuration. When EP is set to a value other than None, it is EP, not BP, which determines the master VIP address. Available settings function as follows:

- NONE - No tracking. EP = BP
- ALL - If the status of all virtual servers is UP, EP = BP. Otherwise, EP = 0.
- ONE - If the status of at least one virtual server is UP, EP = BP. Otherwise, EP = 0.
- PROGRESSIVE - If the status of all virtual servers is UP, EP = BP. If the status of all virtual servers is DOWN, EP = 0. Otherwise EP = BP (1 - K/N), where N is the total number of virtual servers associated with the VIP address and K is the number of virtual servers for which the status is DOWN. Default: NONE.

flags Flags.

IPAddress The IP address bound to the VRID.

state State of this VRID.

stateflag operationalOwnerNode Run time owner node of the vrid.

ownerNode In a cluster setup, assign a cluster node as the owner of this VMAC address for IP based VRRP configuration. If no owner is configured, owner node is displayed as ALL and one node is dynamically elected as the owner.

trackifNum Interfaces which need to be tracked for this vrID.

trackifNumPriority Priority by which the Effective priority will be reduced if any of the tracked interfaces goes down in an active-active configuration.

preemptiondelaytimer Preemption delay time, in seconds, in an active-active configuration. If any high priority node will come in network, it will wait for these many seconds before becoming master.

devno count

Example

show vrid

bind vrID

Binds the specified interfaces to a VMAC configuration.

Synopsis

bind vrID <id> (-ifnum <interface_name> ... | -trackifNum <interface_name> ...)

Arguments

id Integer that uniquely identifies the VMAC address. The generic VMAC address is in the form of 00:00:5e:00:01:<VRID>. For example, if you add a VRID with a value of 60 and bind it to an interface, the resulting VMAC address is 00:00:5e:00:01:3c, where 3c is the hexadecimal representation of 60. Minimum value: 1 Maximum value: 255

ifnum Interfaces to bind to the VMAC. Use spaces to separate multiple entries. For a Citrix ADC, specify the interface in C/U notation (for example, 1/3).For a cluster setup for configuring interface based VRRP, specify the interface in N/C/U notation (for example, 2/1/3) . where C can take one of the following values:

- 0 - Indicates a mgmt port.
- 1 - Indicates a 1 Gbps port.
- 10 - Indicates a 10 Gbps port. Note: Interface based VRRP is only applicable to a two-node cluster where one of node is in active state and the other in Spare. You must associate the VRID to the interfaces of both the nodes of the active-spare cluster setup. This is because unlike in a high availability setup, interface ID differs in a cluster setup

trackifNum Interfaces which need to be tracked for this vrID.

Example

add vrID 1

unset vrID

Use this command to remove vrID settings.Refer to the set vrID command for meanings of the arguments.

Synopsis

unset vrID <id>

unbind vrID

Unbinds specified interfaces from a VMAC configuration.

Synopsis

unbind vrID <id> (-ifnum <interface_name> ... | -trackifNum <interface_name> ...)

Arguments

id Integer value that uniquely identifies the VMAC address. The generic VMAC address is in the form of 00:00:5e:00:01:<VRID>. For example, if you add a VRID with a value of 60 and bind it to an interface, the resulting VMAC address is 00:00:5e:00:01:3c, where 3c is the hexadecimal representation of 60. Minimum value: 1 Maximum value: 255

ifnum Interfaces to unbind from the VMAC, specified in (slot/port) notation (for example, 1/2). Use spaces to separate multiple entries.

trackifNum Interfaces which need to be tracked for this vrID.

set vrID

Modifies parameters related to a VMAC address on the Citrix ADC.

Synopsis

set vrID <id>

Arguments

id Integer value that uniquely identifies the VMAC address. The generic VMACaddressis in the form of 00:00:5e:00:01:<VRID>. For example, if you add a VRID with a value of 60 and bind it to an interface, the resulting VMAC address is 00:00:5e:00:01:3c, where 3c is the hexadecimal representation of 60. Minimum value: 1 Maximum value: 255

priority Base priority (BP), in an active-active mode configuration, which ordinarily determines the master VIP address. Default value: 255 Minimum value: 0 Maximum value: 255

preemption In an active-active mode configuration, make a backup VIP address the master if its priority becomes higher than that of a master VIP address bound to this VMAC address. If you

disable pre-emption while a backup VIP address is the master, the backup VIP address remains master until the original master VIP's priority becomes higher than that of the current master.

Possible values: ENABLED, DISABLED Default value: ENABLED

sharing In an active-active mode configuration, enable the backup VIP address to process any traffic instead of dropping it.

Possible values: ENABLED, DISABLED Default value: DISABLED

tracking The effective priority (EP) value, relative to the base priority (BP) value in an active-active mode configuration. When EP is set to a value other than None, it is EP, not BP, which determines the master VIP address. Available settings function as follows:

- NONE - No tracking. EP = BP
- ALL - If the status of all virtual servers is UP, EP = BP. Otherwise, EP = 0.
- ONE - If the status of at least one virtual server is UP, EP = BP. Otherwise, EP = 0.
- PROGRESSIVE - If the status of all virtual servers is UP, EP = BP. If the status of all virtual servers is DOWN, EP = 0. Otherwise EP = BP (1 - K/N), where N is the total number of virtual servers associated with the VIP address and K is the number of virtual servers for which the status is DOWN. Default: NONE.

Possible values: NONE, ONE, ALL, PROGRESSIVE Default value: NONE

ownerNode In a cluster setup, assign a cluster node as the owner of this VMAC address for IP based VRRP configuration. If no owner is configured, owner node is displayed as ALL and one node is dynamically elected as the owner. Default value: -1 Minimum value: 0 Maximum value: 31

trackifNumPriority Priority by which the Effective priority will be reduced if any of the tracked interfaces goes down. Default value: 0 Minimum value: 1 Maximum value: 255

preemptiondelaytimer Preemption delay time, in seconds, in an active-active configuration. If any high priority node will come in network, it will wait for these many seconds before becoming master. Default value: 0 Minimum value: 1 Maximum value: 36000

Example

set vrID 1 -priority 100

rm vrID

Removes a specified VMAC entry or all VMAC entries from the Citrix ADC.

Synopsis

rm vrID (<id> | -all)

Arguments

id Integer value that uniquely identifies the VMAC address. Minimum value: 1 Maximum value: 255

all Remove all the configured VMAC addresses from the Citrix ADC.

add vrID

Adds a VMAC address to the Citrix ADC. A Virtual MAC address (VMAC) is a floating entity, shared by the nodes in an high availability, or active-active, or cluster setup

Synopsis

add vrID <id>

Arguments

id Integer that uniquely identifies the VMAC address. The generic VMAC address is in the form of 00:00:5e:00:01:<VRID>. For example, if you add a VRID with a value of 60 and bind it to an interface, the resulting VMAC address is 00:00:5e:00:01:3c, where 3c is the hexadecimal representation of 60. Minimum value: 1 Maximum value: 255

priority Base priority (BP), in an active-active mode configuration, which ordinarily determines the master VIP address. Default value: 255 Minimum value: 0 Maximum value: 255

preemption In an active-active mode configuration, make a backup VIP address the master if its priority becomes higher than that of a master VIP address bound to this VMAC address. If you disable pre-emption while a backup VIP address is the master, the backup VIP address remains master until the original master VIP's priority becomes higher than that of the current master.

Possible values: ENABLED, DISABLED Default value: ENABLED

sharing In an active-active mode configuration, enable the backup VIP address to process any traffic instead of dropping it.

Possible values: ENABLED, DISABLED Default value: DISABLED

tracking The effective priority (EP) value, relative to the base priority (BP) value in an active-active mode configuration. When EP is set to a value other than None, it is EP, not BP, which determines the master VIP address. Available settings function as follows:

- NONE - No tracking. EP = BP
- ALL - If the status of all virtual servers is UP, EP = BP. Otherwise, EP = 0.
- ONE - If the status of at least one virtual server is UP, EP = BP. Otherwise, EP = 0.
- PROGRESSIVE - If the status of all virtual servers is UP, EP = BP. If the status of all virtual servers is DOWN, EP = 0. Otherwise EP = BP (1 - K/N), where N is the total number of virtual servers associated with the VIP address and K is the number of virtual servers for which the status is DOWN. Default: NONE.

Possible values: NONE, ONE, ALL, PROGRESSIVE Default value: NONE

ownerNode In a cluster setup, assign a cluster node as the owner of this VMAC address for IP based VRRP configuration. If no owner is configured, owner node is displayed as ALL and one node is dynamically elected as the owner. Default value: -1 Minimum value: 0 Maximum value: 31

trackifNumPriority Priority by which the Effective priority will be reduced if any of the tracked interfaces goes down in an active-active configuration. Default value: 0 Minimum value: 1 Maximum value: 255

preemptiondelaytimer Preemption delay time, in seconds, in an active-active configuration. If any high priority node will come in network, it will wait for these many seconds before becoming master. Default value: 0 Minimum value: 1 Maximum value: 36000

Example

add vrID 1

vrID6

The following operations can be performed on "vrID6":

unbind| rm| set| show| unset| add| bind|

unbind vrID6

Unbinds the specified interfaces from a VMAC6 configuration.

Synopsis

unbind vrID6 <id> (-ifnum <interface_name> ... | -trackifNum <interface_name> ...)

Arguments

id Integer value that uniquely identifies a VMAC6 address. Minimum value: 1 Maximum value: 255

ifnum Interfaces to unbind from the VMAC6, specified in (slot/port) notation (for example, 1/2). Use spaces to separate multiple entries.

trackifNum Interfaces which need to be tracked for this vrID.

rm vrID6

Removes a specified VMAC6 entry or all VMAC6 entries from the Citrix ADC.

Synopsis

rm vrID6 (<id> | -all)

Arguments

id Integer value that uniquely identifies a VMAC6 address. Minimum value: 1 Maximum value: 255

all Remove all configured VMAC6 addresses from the Citrix ADC.

set vrID6

Modifies parameters related to a VMAC address on the Citrix ADC.

Synopsis

set vrID6 <id>

Arguments

id Integer value that uniquely identifies the VMAC address. The generic VMACaddress is in the form of 00:00:5e:00:01:<VRID>. For example, if you add a VRID with a value of 60 and bind it to an interface, the resulting VMAC address is 00:00:5e:00:01:3c, where 3c is the hexadecimal representation of 60. Minimum value: 1 Maximum value: 255

priority Base priority (BP), in an active-active mode configuration, which ordinarily determines the master VIP address. Default value: 255 Minimum value: 0 Maximum value: 255

preemption In an active-active mode configuration, make a backup VIP address the master if its priority becomes higher than that of a master VIP address bound to this VMAC address. If you disable pre-emption while a backup VIP address is the master, the backup VIP address remains master until the original master VIP's priority becomes higher than that of the current master.

Possible values: ENABLED, DISABLED Default value: ENABLED

sharing In an active-active mode configuration, enable the backup VIP address to process any traffic instead of dropping it.

Possible values: ENABLED, DISABLED Default value: DISABLED

tracking The effective priority (EP) value, relative to the base priority (BP) value in an active-active mode configuration. When EP is set to a value other than None, it is EP, not BP, which determines the master VIP address. Available settings function as follows:

- NONE - No tracking. EP = BP
- ALL - If the status of all virtual servers is UP, EP = BP. Otherwise, EP = 0.
- ONE - If the status of at least one virtual server is UP, EP = BP. Otherwise, EP = 0.
- PROGRESSIVE - If the status of all virtual servers is UP, EP = BP. If the status of all virtual servers is DOWN, EP = 0. Otherwise EP = BP (1 - K/N), where N is the total number of virtual servers associated with the VIP address and K is the number of virtual servers for which the status is DOWN. Default: NONE.

Possible values: NONE, ONE, ALL, PROGRESSIVE Default value: NONE

preemptiondelaytimer Preemption delay time in seconds, in an active-active configuration. If any high priority node will come in network, it will wait for these many seconds before becoming master. Default value: 0 Minimum value: 1 Maximum value: 36000

trackifNumPriority Priority by which the Effective priority will be reduced if any of the tracked interfaces goes down in an active-active configuration. Default value: 0 Minimum value: 1 Maximum value: 255

ownerNode In a cluster setup, assign a cluster node as the owner of this VMAC address for IP based VRRP configuration. If no owner is configured, ow ner node is displayed as ALL and one node is dynamically elected as the owner. Default value: -1 Minimum value: 0 Maximum value: 31

Example

set vrID6 1 -priority 100

show vrID6

Displays the settings of all VRID6s configured on the Citrix ADC, or of the specified VRID6. To display the settings of all the VRID6s, run the command without any parameters. To display the settings of a particular VRID6, specify the VRID6.

Synopsis

show vrID6

Arguments

id Integer value that uniquely identifies a VMAC6 address. Minimum value: 1 Maximum value: 255

Output

ifaces Interfaces bound to this VRID.

ifnum Interfaces to bind to the VMAC6, specified in (slot/port) notation (for example, 1/2).Use spaces to separate multiple entries.

type Type (static or dynamic) of this VRID.

vlan The VLAN in which this VRID resides.

priority Base priority (BP), in an active-active mode configuration, which ordinarily determines the master VIP address.

state State of this VRID.

flags Flags.

stateflag IPAddress The IP address bound to the VRID6

preemption In an active-active mode configuration, make a backup VIP address the master if its priority becomes higher than that of a master VIP address bound to this VMAC address. If you disable pre-emption while a backup VIP address is the master, the backup VIP address remains master until the original master VIP's priority becomes higher than that of the current master.

sharing In an active-active mode configuration, enable the backup VIP address to process any traffic instead of dropping it.

preemptiondelaytimer Preemption delay time in seconds, in an active-active configuration. If any high priority node will come in network, it will wait for these many seconds before becoming master.

trackifNum Interfaces which need to be tracked for this vrID.

trackifNumPriority Priority by which the Effective priority will be reduced if any of the tracked interfaces goes down in an active-active configuration.

effectivePriority The effective priority of this VRID.

tracking The effective priority (EP) value, relative to the base priority (BP) value in an active-active mode configuration. When EP is set to a value other than None, it is EP, not BP, which determines the master VIP address. Available settings function as follows:

- NONE - No tracking. EP = BP
- ALL - If the status of all virtual servers is UP, EP = BP. Otherwise, EP = 0.
- ONE - If the status of at least one virtual server is UP, EP = BP. Otherwise, EP = 0.
- PROGRESSIVE - If the status of all virtual servers is UP, EP = BP. If the status of all virtual servers is DOWN, EP = 0. Otherwise EP = BP (1 - K/N), where N is the total number of virtual servers associated with the VIP address and K is the number of virtual servers for which the status is DOWN. Default: NONE.

operationalOwnerNode Run time owner node of the vrid.

ownerNode In a cluster setup, assign a cluster node as the owner of this VMAC address for IP based VRRP configuration. If no owner is configured, ow ner node is displayed as ALL and one node is dynamically elected as the owner.

devno count

Example

show vrid6

unset vrID6

Use this command to remove vrID6 settings.Refer to the set vrID6 command for meanings of the arguments.

Synopsis

unset vrID6 <id>

add vrID6

Adds a VMAC6 address to the Citrix ADC. A Virtual MAC address (VMAC6) is a floating entity, shared by the nodes in a high availability, or active-active, or cluster setup.

Synopsis

add vrID6 <id>

Arguments

id Integer value that uniquely identifies a VMAC6 address. Minimum value: 1 Maximum value: 255

priority Base priority (BP), in an active-active mode configuration, which ordinarily determines the master VIP address. Default value: 255 Minimum value: 0 Maximum value: 255

preemption In an active-active mode configuration, make a backup VIP address the master if its priority becomes higher than that of a master VIP address bound to this VMAC address. If you disable pre-emption while a backup VIP address is the master, the backup VIP address remains master until the original master VIP's priority becomes higher than that of the current master.

Possible values: ENABLED, DISABLED Default value: ENABLED

sharing In an active-active mode configuration, enable the backup VIP address to process any traffic instead of dropping it.

Possible values: ENABLED, DISABLED Default value: DISABLED

tracking The effective priority (EP) value, relative to the base priority (BP) value in an active-active mode configuration. When EP is set to a value other than None, it is EP, not BP, which determines the master VIP address. Available settings function as follows:

- NONE - No tracking. EP = BP
- ALL - If the status of all virtual servers is UP, EP = BP. Otherwise, EP = 0.
- ONE - If the status of at least one virtual server is UP, EP = BP. Otherwise, EP = 0.
- PROGRESSIVE - If the status of all virtual servers is UP, EP = BP. If the status of all virtual servers is DOWN, EP = 0. Otherwise EP = BP (1 - K/N), where N is the total number of virtual servers associated with the VIP address and K is the number of virtual servers for which the status is DOWN. Default: NONE.

Possible values: NONE, ONE, ALL, PROGRESSIVE Default value: NONE

preemptiondelaytimer Preemption delay time in seconds, in an active-active configuration. If any high priority node will come in network, it will wait for these many seconds before becoming master. Default value: 0 Minimum value: 1 Maximum value: 36000

trackifNumPriority Priority by which the Effective priority will be reduced if any of the tracked interfaces goes down in an active-active configuration. Default value: 0 Minimum value: 1 Maximum value: 255

ownerNode In a cluster setup, assign a cluster node as the owner of this VMAC address for IP based VRRP configuration. If no owner is configured, ow ner node is displayed as ALL and one node is dynamically elected as the owner. Default value: -1 Minimum value: 0 Maximum value: 31

Example

add vrID6 1

bind vrID6

Binds the specified interfaces to a VMAC6 configuration.

Synopsis

bind vrID6 <id> (-ifnum <interface_name> ... | -trackifNum <interface_name> ...)

Arguments

id Integer value that uniquely identifies a VMAC6 address. Minimum value: 1 Maximum value: 255

ifnum Interfaces to bind to the VMAC. Use spaces to separate multiple entries. For a Citrix ADC, specify the interface in C/U notation (for example, 1/3).For a cluster setup for configuring interface based VRRP, specify the interface in N/C/U notation(for example, 2/1/3) . where C can take one of the following values:

```
-  0 - Indicates a mgmt port.

-  1 - Indicates a 1 Gbps port.

-  10 - Indicates a 10 Gbps port.
```

Note: Interface based VRRP is only applicable to a two-node cluster where one of node is in active state and the other in Spare. You must associate the VRID to the interfaces of both the nodes of the active-spare cluster setup. This is because unlike in a high availability setup, interface ID differs in a cluster setup.

trackifNum Interfaces which need to be tracked for this vrID.

Example

add vrID6 1

vrIDParam

The following operations can be performed on "vrIDParam":

show| unset| set|

show vrIDParam

Displays the VRID global settings on the Citrix ADC.

Synopsis

show vrIDParam

Arguments

Output

sendToMaster Forward packets to the master node, in an active-active mode configuration, if the virtual server is in the backup state and sharing is disabled.

helloInterval Interval, in milliseconds, between vrrp advertisement messages sent to the peer node in active-active mode.

deadInterval Number of seconds after which a peer node in active-active mode is marked down if vrrp advertisements are not received from the peer node.

unset vrIDParam

Use this command to remove vrIDParam settings.Refer to the set vrIDParam command for meanings of the arguments.

Synopsis

unset vrIDParam

set vrIDParam

Sets global parameters of VMACs on the Citrix ADC.

Synopsis

set vrIDParam

Arguments

sendToMaster Forward packets to the master node, in an active-active mode configuration, if the virtual server is in the backup state and sharing is disabled.

Possible values: ENABLED, DISABLED Default value: DISABLED

helloInterval Interval, in milliseconds, between vrrp advertisement messages sent to the peer node in active-active mode. Default value: 1000 Minimum value: 200 Maximum value: 1000

deadInterval Number of seconds after which a peer node in active-active mode is marked down if vrrp advertisements are not received from the peer node. Default value: 3 Minimum value: 1 Maximum value: 60

Example

set vrIDParam -sendToMaster ENABLED

Related Commands

- add vrid6

vxlan

The following operations can be performed on "vxlan":

unbind| rm| show| set| unset| bind| stat| add|

unbind vxlan

Unbinds tunnels and IP addresses from the VXLAN

Synopsis

unbind vxlan <id> [-IPAddress <ip_addr|ipv6_addr|*>]

Arguments

id A positive integer, which is also called VXLAN Network Identifier (VNI), that uniquely identifies a VXLAN. Minimum value: 1 Maximum value: 16777215

srcIP The source IP address to use in outgoing vxlan packets.

IPAddress The IP Address associated with the VXLAN configuration.

netmask Subnet mask for the network address defined for this VXLAN.

Example

unbind vxlan 20000 -tunnel t1

rm vxlan

Removes a VXLAN from the Citrix ADC

Synopsis

rm vxlan <id>

Arguments

id A positive integer, which is also called VXLAN Network Identifier (VNI), that uniquely identifies a VXLAN. Minimum value: 1 Maximum value: 16777215

Example

rm vxlan 20000

show vxlan

Display all the VXLANs on the Citrix ADC

Synopsis

show vxlan

Arguments

id A positive integer, which is also called VXLAN Network Identifier (VNI), that uniquely identifies a VXLAN. Minimum value: 1 Maximum value: 16777215

Output

vlan ID of VLANs whose traffic is allowed over this VXLAN. If you do not specify any VLAN IDs, the Citrix ADC allows traffic of all VLANs that are not part of any other VXLANs.

port Specifies UDP destination port for VXLAN packets.

dynamicRouting Enable dynamic routing on this VXLAN.

ipv6DynamicRouting Enable all IPv6 dynamic routing protocols on this VXLAN. Note: For the ENABLED setting to work, you must configure IPv6 dynamic routing protocols from the VTYSH command line.

innerVlanTagging Specifies whether Citrix ADC should generate VXLAN packets with inner VLAN tag.

tunnel Specifies the name of the configured tunnel to be associated with this VXLAN.

IPAddress The IP address assigned to the VXLAN.

netmask Subnet mask for the network address defined for this VXLAN.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

type VXLAN encapsulation type. VXLAN, VXLANGPE

protocol VXLAN-GPE next protocol. RESERVED, IPv4, IPv6, ETHERNET, NSH

stateflag Internal flag for display

partitionName The Partition to which this vxlan is bound

srcIP The source IP address to use in outgoing vxlan packets.

devno count

set vxlan

Modify VXLAN parameters

Synopsis

set vxlan <id>

Arguments

id A positive integer, which is also called VXLAN Network Identifier (VNI), that uniquely identifies a VXLAN. Minimum value: 1 Maximum value: 16777215

vlan ID of VLANs whose traffic is allowed over this VXLAN. If you do not specify any VLAN IDs, the Citrix ADC allows traffic of all VLANs that are not part of any other VXLANs. Minimum value: 2 Maximum value: 4094

port Specifies UDP destination port for VXLAN packets. Default value: 4789 Minimum value: 1 Maximum value: 65534

dynamicRouting Enable dynamic routing on this VXLAN.

Possible values: ENABLED, DISABLED Default value: DISABLED

ipv6DynamicRouting Enable all IPv6 dynamic routing protocols on this VXLAN. Note: For the ENABLED setting to work, you must configure IPv6 dynamic routing protocols from the VTYSH command line.

Possible values: ENABLED, DISABLED Default value: DISABLED

innerVlanTagging Specifies whether Citrix ADC should generate VXLAN packets with inner VLAN tag.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set vxlan 20000 -vlan 4

unset vxlan

Use this command to remove vxlan settings.Refer to the set vxlan command for meanings of the arguments.

Synopsis

unset vxlan <id>

bind vxlan

Binds tunnels or IP addresses to the VXLAN

Synopsis

bind vxlan <id> [-IPAddress <ip_addr|ipv6_addr|*>]

Arguments

id A positive integer, which is also called VXLAN Network Identifier (VNI), that uniquely identifies a VXLAN. Minimum value: 1 Maximum value: 16777215

srcIP The source IP address to use in outgoing vxlan packets.

IPAddress Network address to be associated with the VXLAN. Should exist on the appliance before you associate it with the VXLAN.

netmask Subnet mask for the network address defined for this VXLAN.

Example

bind vxlan 20000 -tunnel t1

stat vxlan

Display statistics for VXLAN(s).

Synopsis

stat vxlan

Arguments

id An integer specifying the VXLAN identification number (VNID). Minimum value: 1 Maximum value: 16777215

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Packets received (RxPkts) Packets received on the VXLAN.

Bytes received (RxBytes) Bytes of data received on the VXLAN.

Packets sent (TxPkts) Packets transmitted on the VXLAN.

Bytes sent (TxBytes) Bytes of data transmitted on the VXLAN.

Example

stat vxlan 10000

Related Commands

- stat MapDomain

add vxlan

Adds a VXLAN to the Citrix ADC.

Synopsis

add vxlan <id> [-type (VXLAN | VXLANGPE)]

Arguments

id A positive integer, which is also called VXLAN Network Identifier (VNI), that uniquely identifies a VXLAN. Minimum value: 1 Maximum value: 16777215

vlan ID of VLANs whose traffic is allowed over this VXLAN. If you do not specify any VLAN IDs, the Citrix ADC allows traffic of all VLANs that are not part of any other VXLANs. Minimum value: 2 Maximum value: 4094

port Specifies UDP destination port for VXLAN packets. Default value: 4789 Minimum value: 1 Maximum value: 65534

dynamicRouting Enable dynamic routing on this VXLAN.

Possible values: ENABLED, DISABLED Default value: DISABLED

ipv6DynamicRouting Enable all IPv6 dynamic routing protocols on this VXLAN. Note: For the ENABLED setting to work, you must configure IPv6 dynamic routing protocols from the VTYSH command line.

Possible values: ENABLED, DISABLED Default value: DISABLED

type VXLAN encapsulation type. VXLAN, VXLANGPE

Possible values: VXLAN, VXLANGPE Default value: VXLAN

protocol VXLAN-GPE next protocol. RESERVED, IPv4, IPv6, ETHERNET, NSH

Possible values: IPv4, IPv6, ETHERNET, NSH Default value: ETHERNET

innerVlanTagging Specifies whether Citrix ADC should generate VXLAN packets with inner VLAN tag.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

add vxlan 20000 -vlan 4

vxlanVlanMap

The following operations can be performed on "vxlanVlanMap":

unbind| show| rm| add| bind|

unbind vxlanVlanMap

Remove a vlan to vxlan mappings.

Synopsis

unbind vxlanVlanMap <name> -vxlan <positive_integer>

Arguments

name Name of the mapping table.

vxlan The VXLAN assigned to the vlan inside the cloud. Minimum value: 1 Maximum value: 16777215

Example

unbind vxlanVlanMap table1 -vxlan 3000

show vxlanVlanMap

Retrieve vlan to vxlan mappings.

Synopsis

show vxlanVlanMap

Arguments

name Name of the mapping table.

Output

stateflag Internal flag for display

vxlan The VXLAN assigned to the vlan inside the cloud.

vlan The vlan id or the range of vlan ids in the on-premise network.

devno count

Example

show vxlanVlanMap

rm vxlanVlanMap

Delete the vlan to vxlan mapping table.

Synopsis

rm vxlanVlanMap <name>

Arguments

name Name of the mapping table.

Example

rm vxlanVlanMap table1

add vxlanVlanMap

Add a table that gives a vlan to vxlan mapping.

Synopsis

add vxlanVlanMap <name>

Arguments

name Name of the mapping table.

Example

add vxlanVlanMap table1

bind vxlanVlanMap

Specify vlan to vxlan mappings.

Synopsis

bind vxlanVlanMap <name> [-vxlan <positive_integer> -vlan <int> ...]

Arguments

name Name of the mapping table.

vxlan The VXLAN assigned to the vlan inside the cloud. Minimum value: 1 Maximum value: 16777215

vlan The vlan id or the range of vlan ids in the on-premise network. Minimum value: 1 Maximum value: 4094

Example

bind vxlanVlanMap tab1 -vxlan 7000 -vlan 7 9 100-800

ns

ns-acl

The following operations can be performed on "ns-acl":

stat| set| add| unset| disable| rm| enable| rename| show|

stat ns acl

Displays statistics related to the extended ACL rules. To display statistics of all the extended ACL rules, run the command without any parameters. To display statistics of a particular extended ACL rule, specify the name of the extended ACL rule.

Synopsis

stat ns acl

Arguments

aclname Name of the extended ACL rule whose statistics you want the Citrix ADC to display.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Bridge ACL hits (ACLBdg) Packets matching a bridge ACL, which is in transparent mode and bypasses service processing.

Deny ACL hits (ACLDeny) Packets dropped because they match ACLs with processing mode set to DENY.

Allow ACL hits (ACLAllow) Packets matching ACLs with processing mode set to ALLOW. Citrix ADC processes these packets.

NAT ACL hits (ACLNAT) Packets matching a NAT ACL, resulting in a NAT session.

ACL hits (ACLHits) Packets matching an ACL.

ACL misses (ACLMiss) Packets not matching any ACL.

ACL Count (ACLCount) Total number of ACL rules configured.

Effective ACL Count (EffectiveACLCount) Total number of Effective ACL rules configured.

DFD ACL hits (dfdACLHits) Packets matching an dfd ACL.

DFD ACL misses (dfdACLMiss) Packets not matching any DFD ACL.

DFD ACL Count (dfdACLCount) Total number of DFD ACL rules configured.

Hits for this ACL (Hits) Number of times the acl was hit

Example

stat acl

Related Commands

- stat ns partition

set ns acl

Modifies the parameters of an ACL rule. To commit this operation, you must apply the extended ACLs.

Synopsis

set ns acl <aclname> [-srcIP <srcIPVal>] [-srcPort <srcPortVal>] [-destIP <destIPVal>] [-destPort <destPortVal>] [-srcMac <mac_addr>] [-icmpType <positive_integer>]

Arguments

aclname Name of the ACL rule whose parameters you want to modify.

aclaction Action to perform on incoming IPv4 packets that match the extended ACL rule. Available settings function as follows:

- ALLOW - The Citrix ADC processes the packet.
- BRIDGE - The Citrix ADC bridges the packet to the destination without processing it.
- DENY - The Citrix ADC drops the packet.

Possible values: BRIDGE, DENY, ALLOW

srcIP IP address or range of IP addresses to match against the source IP address of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

srcIPVal IP address or range of IP addresses to match against the source IP address of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example:10.102.29.30-10.102.29.189.

srcPort Port number or range of port numbers to match against the source port number of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

srcPortVal Port number or range of port numbers to match against the source port number of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90. Maximum value: 65535

destIP IP address or range of IP addresses to match against the destination IP address of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

destIPVal IP address or range of IP addresses to match against the destination IP address of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.

destPort Port number or range of port numbers to match against the destination port number of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

destPortVal Port number or range of port numbers to match against the destination port number of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols. Maximum value: 65535

srcMac MAC address to match against the source MAC address of an incoming IPv4 packet.

srcMacMask Used to define range of Source MAC address. It takes string of 0 and 1, 0s are for exact match and 1s for wildcard. For matching first 3 bytes of MAC address, srcMacMask value "000000111111". Default value: "000000000000"

protocol Protocol to match against the protocol of an incoming IPv4 packet.

Possible values: ICMP, IGMP, TCP, EGP, IGP, ARGUS, UDP, RDP, RSVP, EIGRP, L2TP, ISIS, GGP, IPoverIP, ST, CBT, BBN-RCC-M, NVP-II, PUP, EMCON, XNET, CHAOS, MUX, DCN-MEAS, HMP, PRM, XNS-IDP, TRUNK-1, TRUNK-2, LEAF-1, LEAF-2, IRTP, ISO-TP4, NETBLT, MFE-NSP, MERIT-INP, SEP, 3PC, IDPR, XTP, DDP, IDPR-CMTP, TP++, IL, IPv6, SDRP, IPv6-Route, IPv6-Frag, IDRP, GRE, MHRP, BNA, ESP, AH, I-NLSP, SWIPE, NARP, MOBILE, TLSP, SKIP, ICMPV6, IPv6-NoNx, IPv6-Opts, Any-Host-Internal-Protocol, CFTP, Any-Local-Network, SAT-EXPAK, KRYPTOLAN, RVD, IPPC, Any-Distributed-File-System, TFTP, VISA, IPCV, CPNX, CPHB, WSN, PVP, BR-SAT-MO, SUN-ND, WB-MON, WB-EXPAK, ISO-IP, VMTP, SECURE-VM, VINES, TTP, NSFNET-IG, DGP, TCF, OSPFIGP, Sprite-RP, LARP, MTP, AX.25, IPIP, MICP, SCC-SP, ETHERIP, Any-Private-Encryption-Scheme, GMTP, IFMP, PNNI, PIM, ARIS, SCPS, QNX, A/N, IPComp, SNP, Compaq-Pe, IPX-in-IP, VRRP, PGM, Any-0-Hop-Protocol, ENCAP, DDX, IATP, STP, SRP, UTI,

SMP, SM, PTP, FIRE, CRTP, CRUDP, SSCOPMCE, IPLT, SPS, PIPE, SCTP, FC, RSVP-E2E-IGNORE, Mobility-Header, UDPLite

protocolNumber Protocol to match against the protocol of an incoming IPv4 packet. Minimum value: 1 Maximum value: 255

icmpType ICMP Message type to match against the message type of an incoming ICMP packet. For example, to block DESTINATION UNREACHABLE messages, you must specify 3 as the ICMP type.

Note: This parameter can be specified only for the ICMP protocol. Minimum value: 0 Maximum value: 65536

icmpCode Code of a particular ICMP message type to match against the ICMP code of an incoming ICMP packet. For example, to block DESTINATION HOST UNREACHABLE messages, specify 3 as the ICMP type and 1 as the ICMP code.

If you set this parameter, you must set the ICMP Type parameter. Minimum value: 0 Maximum value: 65536

vlan ID of the VLAN. The Citrix ADC applies the ACL rule only to the incoming packets of the specified VLAN. If you do not specify a VLAN ID, the appliance applies the ACL rule to the incoming packets on all VLANs. Minimum value: 1 Maximum value: 4094

vxlan ID of the VXLAN. The Citrix ADC applies the ACL rule only to the incoming packets of the specified VXLAN. If you do not specify a VXLAN ID, the appliance applies the ACL rule to the incoming packets on all VXLANs. Minimum value: 1 Maximum value: 16777215

interface ID of an interface. The Citrix ADC applies the ACL rule only to the incoming packets from the specified interface. If you do not specify any value, the appliance applies the ACL rule to the incoming packets of all interfaces.

priority Priority for the extended ACL rule that determines the order in which it is evaluated relative to the other extended ACL rules. If you do not specify priorities while creating extended ACL rules, the ACL rules are evaluated in the order in which they are created. Minimum value: 1 Maximum value: 100000

logstate Enable or disable logging of events related to the extended ACL rule. The log messages are stored in the configured syslog or auditlog server.

Possible values: ENABLED, DISABLED Default value: DISABLED

ratelimit Maximum number of log messages to be generated per second. If you set this parameter, you must enable the Log State parameter. Default value: 100 Minimum value: 1 Maximum value: 10000

established Allow only incoming TCP packets that have the ACK or RST bit set, if the action set for the ACL rule is ALLOW and these packets match the other conditions in the ACL rule.

dfdhash Specifies the type hashmethod to be applied, to steer the packet to the FP of the packet.

Possible values: SIP-SPORT-DIP-DPORT, SIP, DIP, SIP-DIP, SIP-SPORT, DIP-DPORT

stateful If stateful option is enabled, transparent sessions are created for the traffic hitting this ACL and not hitting any other features like LB, INAT etc.

Possible values: YES, NO Default value: NO

Example

set ns acl restrict -srcPort 50

Related Commands

- apply acls

add ns acl

Adds an extended ACL rule to the Citrix ADC. To commit this operation, you must apply the extended ACLs. Extended ACL rules filter data packets on the basis of various parameters, such as IP address, source port, action, and protocol.

Synopsis

add ns acl <aclname> <aclaction> [-srcIP (<srcIPVal> | <srcIPDataset>)] [-srcPort (<srcPortVal> | <srcPortDataset>)] [-destIP (<destIPVal> | <destIPDataset>)] [-destPort (<destPortVal> | <destPortDataset>)] (-TTL <positive_integer> | -stateful (YES | NO)) [-srcMac <mac_addr>] [(-protocol <protocol>) | -protocolNumber <positive_integer>] [-icmpType <positive_integer>] [-logstate (ENABLED | DISABLED)] [-type (CLASSIC | DFD)]

Arguments

aclname Name for the extended ACL rule. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

aclaction Action to perform on incoming IPv4 packets that match the extended ACL rule. Available settings function as follows:

- ALLOW - The Citrix ADC processes the packet.
- BRIDGE - The Citrix ADC bridges the packet to the destination without processing it.
- DENY - The Citrix ADC drops the packet.

Possible values: BRIDGE, DENY, ALLOW

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

srcIP IP address or range of IP addresses to match against the source IP address of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

srcIPVal IP address or range of IP addresses to match against the source IP address of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example:10.102.29.30-10.102.29.189.

srcIPDataset Policy dataset which can have multiple IP ranges bound to it.

srcPort Port number or range of port numbers to match against the source port number of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

srcPortVal Port number or range of port numbers to match against the source port number of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90. Maximum value: 65535

srcPortDataset Policy dataset which can have multiple port ranges bound to it.

destIP IP address or range of IP addresses to match against the destination IP address of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

destIPVal IP address or range of IP addresses to match against the destination IP address of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.

destIPDataset Policy dataset which can have multiple IP ranges bound to it.

destPort Port number or range of port numbers to match against the destination port number of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

destPortVal Port number or range of port numbers to match against the destination port number of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols. Maximum value: 65535

destPortDataset Policy dataset which can have multiple port ranges bound to it.

TTL Number of seconds, in multiples of four, after which the extended ACL rule expires. If you do not want the extended ACL rule to expire, do not specify a TTL value. Minimum value: 1 Maximum value: 2147483647

srcMac MAC address to match against the source MAC address of an incoming IPv4 packet.

srcMacMask Used to define range of Source MAC address. It takes string of 0 and 1, 0s are for exact match and 1s for wildcard. For matching first 3 bytes of MAC address, srcMacMask value "000000111111". Default value: "000000000000"

protocol Protocol to match against the protocol of an incoming IPv4 packet.

Possible values: ICMP, IGMP, TCP, EGP, IGP, ARGUS, UDP, RDP, RSVP, EIGRP, L2TP, ISIS, GGP, IPoverIP, ST, CBT, BBN-RCC-M, NVP-II, PUP, EMCON, XNET, CHAOS, MUX, DCN-MEAS, HMP, PRM, XNS-IDP, TRUNK-1, TRUNK-2, LEAF-1, LEAF-2, IRTP, ISO-TP4, NETBLT, MFE-NSP, MERIT-INP, SEP, 3PC, IDPR, XTP, DDP, IDPR-CMTP, TP++, IL, IPv6, SDRP, IPv6-Route, IPv6-Frag, IDRP, GRE, MHRP, BNA, ESP, AH, I-NLSP, SWIPE, NARP, MOBILE, TLSP, SKIP, ICMPV6, IPv6-NoNx, IPv6-Opts, Any-Host-Internal-Protocol, CFTP, Any-Local-Network, SAT-EXPAK, KRYPTOLAN, RVD, IPPC, Any-Distributed-File-System, TFTP, VISA, IPCV, CPNX, CPHB, WSN, PVP, BR-SAT-MO, SUN-ND, WB-MON, WB-EXPAK, ISO-IP, VMTP, SECURE-VM, VINES, TTP, NSFNET-IG, DGP, TCF, OSPFIGP, Sprite-RP, LARP, MTP, AX.25, IPIP, MICP, SCC-SP, ETHERIP, Any-Private-Encryption-Scheme, GMTP, IFMP, PNNI, PIM, ARIS, SCPS, QNX, A/N, IPComp, SNP, Compaq-Pe, IPX-in-IP, VRRP, PGM, Any-0-Hop-Protocol, ENCAP, DDX, IATP, STP, SRP, UTI, SMP, SM, PTP, FIRE, CRTP, CRUDP, SSCOPMCE, IPLT, SPS, PIPE, SCTP, FC, RSVP-E2E-IGNORE, Mobility-Header, UDPLite

protocolNumber Protocol to match against the protocol of an incoming IPv4 packet. Minimum value: 1 Maximum value: 255

vlan ID of the VLAN. The Citrix ADC applies the ACL rule only to the incoming packets of the specified VLAN. If you do not specify a VLAN ID, the appliance applies the ACL rule to the incoming packets on all VLANs. Minimum value: 1 Maximum value: 4094

vxlan ID of the VXLAN. The Citrix ADC applies the ACL rule only to the incoming packets of the specified VXLAN. If you do not specify a VXLAN ID, the appliance applies the ACL rule to the incoming packets on all VXLANs. Minimum value: 1 Maximum value: 16777215

interface ID of an interface. The Citrix ADC applies the ACL rule only to the incoming packets from the specified interface. If you do not specify any value, the appliance applies the ACL rule to the incoming packets of all interfaces.

established Allow only incoming TCP packets that have the ACK or RST bit set, if the action set for the ACL rule is ALLOW and these packets match the other conditions in the ACL rule.

icmpType ICMP Message type to match against the message type of an incoming ICMP packet. For example, to block DESTINATION UNREACHABLE messages, you must specify 3 as the ICMP type.

Note: This parameter can be specified only for the ICMP protocol. Minimum value: 0 Maximum value: 65536

icmpCode Code of a particular ICMP message type to match against the ICMP code of an incoming ICMP packet. For example, to block DESTINATION HOST UNREACHABLE messages, specify 3 as the ICMP type and 1 as the ICMP code.

If you set this parameter, you must set the ICMP Type parameter. Minimum value: 0 Maximum value: 65536

priority Priority for the extended ACL rule that determines the order in which it is evaluated relative to the other extended ACL rules. If you do not specify priorities while creating extended ACL rules, the ACL rules are evaluated in the order in which they are created. Minimum value: 1 Maximum value: 100000

state Enable or disable the extended ACL rule. After you apply the extended ACL rules, the Citrix ADC compares incoming packets against the enabled extended ACL rules.

Possible values: ENABLED, DISABLED Default value: ENABLED

logstate Enable or disable logging of events related to the extended ACL rule. The log messages are stored in the configured syslog or auditlog server.

Possible values: ENABLED, DISABLED Default value: DISABLED

ratelimit Maximum number of log messages to be generated per second. If you set this parameter, you must enable the Log State parameter. Default value: 100 Minimum value: 1 Maximum value: 10000

type Type of the acl ,default will be CLASSIC. Available options as follows:

- CLASSIC - specifies the regular extended acls.
- DFD - cluster specific acls,specifies hashmethod for steering of the packet in cluster .

Possible values: CLASSIC, DFD Default value: CLASSIC

dfdhash Specifies the type hashmethod to be applied, to steer the packet to the FP of the packet.

Possible values: SIP-SPORT-DIP-DPORT, SIP, DIP, SIP-DIP, SIP-SPORT, DIP-DPORT

stateful If stateful option is enabled, transparent sessions are created for the traffic hitting this ACL and not hitting any other features like LB, INAT etc.

Possible values: YES, NO Default value: NO

Example

add ns acl restrict DENY -srcport 45-1024 -destIP 192.168.1.1 -protocol TCP

Related Commands

- apply acls

unset ns acl

Resets the attributes of the specified extended ACL rule. Attributes for which a default value is available revert to their default values. Refer to the set ns acl command for a description of the parameters..Refer to the set ns acl command for meanings of the arguments.

Synopsis

unset ns acl <aclname>

Example

unset ns acl rule1 -srcPort

Related Commands

- apply acls

disable ns acl

Disables an extended ACL rule. To commit this operation, you must apply the extended ACLs. After you apply the ACL rules, the Citrix ADC does not compare incoming packets against the disabled extended ACL rules.

Synopsis

disable ns acl <aclname> ...

Arguments

aclname Name of the extended ACL rule that you want to disable.

Example

disable ns acl foo

Related Commands

- clear acls

rm ns acl

Removes an extended ACL rule from the Citrix ADC. To commit this operation, you must apply the extended ACLs.

Synopsis

rm ns acl <aclname> ...

Arguments

aclname Name of the extended ACL rule that you want to remove.

Example

rm ns acl restrict

Related Commands

- clear acls

enable ns acl

Enables an extended ACL rule. To commit this operation, you must apply the extended ACLs. After you apply the extended ACL rules, the Citrix ADC compares incoming packets against the enabled extended ACL rules.

Synopsis

enable ns acl <aclname> ...

Arguments

aclname Name of the extended ACL rule that you want to enable.

Example

enable ns acl foo

Related Commands

- clear acls

rename ns acl

Renames an extended ACL rule.

Synopsis

rename ns acl <aclname> <newName>

Arguments

aclname Name of the extended ACL rule that you want to rename.

newName New name for the extended ACL rule. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

Example

rename acl rule rule-new

show ns acl

Displays settings related to the extended ACL rules. To display settings of all the extended ACL rules, run the command without any parameters. To display settings of a particular extended ACL rule, specify the name of the extended ACL rule.

Synopsis

show ns acl

Arguments

aclname Name of the extended ACL rule whose details you want the Citrix ADC to display.

type default will display both CLASSIC and DFD

Possible values: CLASSIC, DFD

Output

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

aclaction Action to perform on incoming IPv4 packets that match the extended ACL rule. Available settings function as follows:

- ALLOW - The Citrix ADC processes the packet.
- BRIDGE - The Citrix ADC bridges the packet to the destination without processing it.

- DENY - The Citrix ADC drops the packet.

srcMac MAC address to match against the source MAC address of an incoming IPv4 packet.

srcMacMask Used to define range of Source MAC address. It takes string of 0 and 1, 0s are for exact match and 1s for wildcard. For matching first 3 bytes of MAC address, srcMacMask value "000000111111".

stateflag ACL state flag.

protocol The protocol number in IP header or name.

protocolNumber The protocol number in IP header or name.

srcPortVal Port number or range of port numbers to match against the source port number of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

srcPortDataset Policy dataset which can have multiple port ranges bound to it.

operator Either the equals (=) or does not equal (!=) logical operator.

destPortVal Port number or range of port numbers to match against the destination port number of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols.

destPortDataset Policy dataset which can have multiple port ranges bound to it.

operator Either the equals (=) or does not equal (!=) logical operator.

srcIPVal IP address or range of IP addresses to match against the source IP address of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example:10.102.29.30-10.102.29.189.

srcIPDataset Policy dataset which can have multiple IP ranges bound to it.

operator Either the equals (=) or does not equal (!=) logical operator.

destIPVal IP address or range of IP addresses to match against the destination IP address of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.

operator Either the equals (=) or does not equal (!=) logical operator.

destIPDataset Policy dataset which can have multiple IP ranges bound to it.

vlan ID of the VLAN. The Citrix ADC applies the ACL rule only to the incoming packets of the specified VLAN. If you do not specify a VLAN ID, the appliance applies the ACL rule to the incoming packets on all VLANs.

vxlan ID of the VXLAN. The Citrix ADC applies the ACL rule only to the incoming packets of the specified VXLAN. If you do not specify a VXLAN ID, the appliance applies the ACL rule to the incoming packets on all VXLANs.

state Enable or disable the extended ACL rule. After you apply the extended ACL rules, the Citrix ADC compares incoming packets against the enabled extended ACL rules.

TTL Number of seconds, in multiples of four, after which the extended ACL rule expires. If you do not want the extended ACL rule to expire, do not specify a TTL value.

icmpType ICMP Message type to match against the message type of an incoming ICMP packet. For example, to block DESTINATION UNREACHABLE messages, you must specify 3 as the ICMP type.

Note: This parameter can be specified only for the ICMP protocol.

icmpCode Code of a particular ICMP message type to match against the ICMP code of an incoming ICMP packet. For example, to block DESTINATION HOST UNREACHABLE messages, specify 3 as the ICMP type and 1 as the ICMP code.

If you set this parameter, you must set the ICMP Type parameter.

interface ID of an interface. The Citrix ADC applies the ACL rule only to the incoming packets from the specified interface. If you do not specify any value, the appliance applies the ACL rule to the incoming packets of all interfaces.

hits The hits of this ACL.

established This flag indicates that the ACL should be used for TCP response traffic only.

priority Priority for the extended ACL rule that determines the order in which it is evaluated relative to the other extended ACL rules. If you do not specify priorities while creating extended ACL rules, the ACL rules are evaluated in the order in which they are created.

kernelstate The commit status of the ACL.

logstate Enable or disable logging of events related to the extended ACL rule. The log messages are stored in the configured syslog or auditlog server.

ratelimit Packet rate limit for acl logging

time Time when this acl is applied.

aclassociate ACL linked

dfdhash Specifies the type hashmethod to be applied, to steer the packet to the FP of the packet.

stateful If stateful option is enabled, transparent sessions are created for the traffic hitting this ACL and not hitting any other features like LB, INAT etc.

aclChildcount Number of childs for this ACL.

devno count

Example

sh acl foo Name: foo Action: ALLOW Hits: 0 srcIP = 10.102.1.150 destIP = 202.54.12.47 srcMac: srcMacMask: Protocol: TCP srcPort destPort = 110 Vlan: Interface: Active Status: ENABLED Applied Status: NOTAPPLIED Priority: 1027

ns-acl6

The following operations can be performed on "ns-acl6":

enable| show| stat| set| rm| add| disable| rename| unset|

enable ns acl6

Enables an ACL6 rule. To commit this operation, you must apply the ACL6s.After you apply the ACL6 rules, the Citrix ADC compares incoming IPv6 packets to the enabled ACL6 rules.

Synopsis

enable ns acl6 <acl6name> ...

Arguments

acl6name Name of ACL6 rule that you want to enable.

Example

enable ns acl6 rule1

Related Commands

- clear ns acls6

show ns acl6

Displays settings related to the ACL6 rules. To display settings of all the ACL6 rules, run the command without any parameters. To display settings of a particular ACL6 rule, specify the name of the ACL6 rule.

Synopsis

show ns acl6

Arguments

acl6name Name of the ACL6 rule whose details you want the Citrix ADC to display.

type default will display both CLASSIC and DFD

Possible values: CLASSIC, DFD

Output

acl6action Action to perform on the incoming IPv6 packets that match the ACL6 rule. Available settings function as follows:

- ALLOW - The Citrix ADC processes the packet.
- BRIDGE - The Citrix ADC bridges the packet to the destination without processing it.
- DENY - The Citrix ADC drops the packet.

srcMac MAC address to match against the source MAC address of an incoming IPv6 packet.

srcMacMask Used to define range of Source MAC address. It takes string of 0 and 1, 0s are for exact match and 1s for wildcard. For matching first 3 bytes of MAC address, srcMacMask value "000000111111".

stateflag ACL6 state flag.

protocol Protocol number in IPv6 header or name.

protocolNumber Protocol number in IPv6 header or name.

srcPortVal Source port (range).

operator Either the equals (=) or does not equal (!=) logical operator.

destPortVal Destination port (range).

operator Either the equals (=) or does not equal (!=) logical operator.

srcIPv6Val Source IPv6 address (range).

operator Either the equals (=) or does not equal (!=) logical operator.

destIPv6Val Destination IPv6 address (range).

operator Either the equals (=) or does not equal (!=) logical operator.

vlan ID of the VLAN. The Citrix ADC applies the ACL6 rule only to the incoming packets on the specified VLAN. If you do not specify a VLAN ID, the appliance applies the ACL6 rule to the incoming packets on all VLANs.

vxlan ID of the VXLAN. The Citrix ADC applies the ACL6 rule only to the incoming packets on the specified VXLAN. If you do not specify a VXLAN ID, the appliance applies the ACL6 rule to the incoming packets on all VXLANs.

state State of the ACL6.

kernelstate Commit status of the ACL6.

TTL Time left to expire ACL6 (in seconds).

icmpType ICMP Message type to match against the message type of an incoming IPv6 ICMP packet. For example, to block DESTINATION UNREACHABLE messages, you must specify 3 as the ICMP type.

Note: This parameter can be specified only for the ICMP protocol.

icmpCode Code of a particular ICMP message type to match against the ICMP code of an incoming IPv6 ICMP packet. For example, to block DESTINATION HOST UNREACHABLE messages, specify 3 as the ICMP type and 1 as the ICMP code.

If you set this parameter, you must set the ICMP Type parameter.

interface ID of an interface. The Citrix ADC applies the ACL6 rule only to the incoming packets from the specified interface. If you do not specify any value, the appliance applies the ACL6 rule to the incoming packets from all interfaces.

hits Number of hits of this ACL6.

established This flag indicates that the ACL6 should be used for TCP response traffic only.

priority Priority for the ACL6 rule, which determines the order in which it is evaluated relative to the other ACL6 rules. If you do not specify priorities while creating ACL6 rules, the ACL6 rules are evaluated in the order in which they are created.

logstate Enable or disable logging of events related to the ACL6 rule. The log messages are stored in the configured syslog or auditlog server.

ratelimit Packet rate limit for acl logging

time Time when this acl is applied.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

aclassociate ACL6 linked

dfdhash Specifies the type of hashmethod to be applied, to steer the packet to the FP of the packet.

dfdprefix hashprefix to be applied to SIP/DIP to generate rsshash FP.eg 128 => hash calculated on the complete IP

stateful If stateful option is enabled, transparent sessions are created for the traffic hitting this ACL6 and not hitting any other features like LB, INAT etc.

devno count

Example

show ns acl6 rule1 1)

```
    Name: r1                            Action: DENY

    srcIPv6 = 2001::1

    destIPv6

    srcMac:                             srcMacMask:

    Protocol:
```

```
    Vlan:                           Interface:

    Active Status: ENABLED          Applied Status: NOTAPPLIED

    Priority: 10                    Hits: 0

    TTL:
```

stat ns acl6

Displays statistics related to the ACL6 rules. To display statistics of all the ACL6 rules, run the command without any parameters. To display statistics of a particular ACL6 rule, specify the name of the ACL6 rule.

Synopsis

stat ns acl6

Arguments

acl6name Name of the ACL6 rule whose statistics you want the Citrix ADC to display.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Bridge ACL6 hits (ACL6Bdg) Packets matching a bridge IPv6 ACL, which is in transparent mode and bypasses service processing.

Deny ACL6 hits (ACL6Deny) Packets dropped because they match IPv6 ACLs with processing mode set to DENY.

Allow ACL6 hits (ACL6Allow) Packets matching IPv6 ACLs with processing mode set to ALLOW. Citrix ADC processes these packets.

NAT ACL6 hits (ACL6NAT) Packets matching a NAT ACL6, resulting in a NAT session.

ACL6 hits (ACL6Hits) Packets matching an IPv6 ACL.

ACL6 misses (ACL6Miss) Packets not matching any IPv6 ACL.

NAT64 ACL6 hits (ACL6NAT64) Packets matching a NAT64 ACL6, resulting in a NAT64 translation.

ACL6 Count (ACL6Count) Total number of ACL6 rules configured.

DFD ACL6 Count (dfdACL6Count) Total number of DFD ACL6 rules configured.

DFD ACL6 hits (dfdACL6Hits) Packets matching an dfd ACL6.

DFD ACL6 misses (dfdACL6Miss) Packets not matching any DFD ACL6.

Hits for this ACL6 (Hits) Number of times the acl6 was hit

Example

stat acl6

Related Commands

- stat ns partition

set ns acl6

Modifies the parameters of an ACL6 rule. To commit this operation, you must apply the ACL6s.

Synopsis

set ns acl6 <acl6name> [-srcIPv6 <srcIPv6Val>] [-srcPort <srcPortVal>] [-destIPv6 <destIPv6Val>] [-destPort <destPortVal>] [-srcMac <mac_addr>] [-icmpType <positive_integer>]

Arguments

acl6name Name of the ACL6 rule whose parameters you want to modify.

aclaction Action associated with the ACL6.

Possible values: BRIDGE, DENY, ALLOW

srcIPv6 IP address or range of IP addresses to match against the source IP address of an incoming IPv6 packet. In the command line interface, separate the range with a hyphen.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

srcIPv6Val Source IPv6 address (range).

srcPort Source Port (range).

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

srcPortVal Source port (range). Maximum value: 65535

destIPv6 IP address or range of IP addresses to match against the destination IP address of an incoming IPv6 packet. In the command line interface, separate the range with a hyphen.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

destIPv6Val Destination IPv6 address (range).

destPort Destination Port (range).

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

destPortVal Destination port (range). Maximum value: 65535

srcMac MAC address to match against the source MAC address of an incoming IPv6 packet.

srcMacMask Used to define range of Source MAC address. It takes string of 0 and 1, 0s are for exact match and 1s for wildcard. For matching first 3 bytes of MAC address, srcMacMask value "000000111111". Default value: "000000000000"

protocol Protocol, identified by protocol name, to match against the protocol of an incoming IPv6 packet.

Possible values: ICMPV6, TCP, UDP, ICMP, IGMP, EGP, IGP, ARGUS, RDP, RSVP, EIGRP, L2TP, ISIS, GGP, IPoverIP, ST, CBT, BBN-RCC-M, NVP-II, PUP, EMCON, XNET, CHAOS, MUX, DCN-MEAS, HMP, PRM, XNS-IDP, TRUNK-1, TRUNK-2, LEAF-1, LEAF-2, IRTP, ISO-TP4, NETBLT, MFE-NSP, MERIT-INP, SEP, 3PC, IDPR, XTP, DDP, IDPR-CMTP, TP++, IL, IPv6, SDRP, IPv6-Route, IPv6-Frag, IDRP, GRE, MHRP, BNA, ESP, AH, I-NLSP, SWIPE, NARP, MOBILE, TLSP, SKIP, IPv6-NoNx, IPv6-Opts, Any-Host-Internal-Protocol, CFTP, Any-Local-Network, SAT-EXPAK, KRYPTOLAN, RVD, IPPC, Any-Distributed-File-System, TFTP, VISA, IPCV, CPNX, CPHB, WSN, PVP, BR-SAT-MO, SUN-ND, WB-MON, WB-EXPAK, ISO-IP, VMTP, SECURE-VM, VINES, TTP, NSFNET-IG, DGP, TCF, OSPFIGP, Sprite-RP, LARP, MTP, AX.25, IPIP, MICP, SCC-SP, ETHERIP, Any-Private-Encryption-Scheme, GMTP, IFMP, PNNI, PIM, ARIS, SCPS, QNX, A/N, IPComp, SNP, Compaq-Pe, IPX-in-IP, VRRP, PGM, Any-0-Hop-Protocol, ENCAP, DDX, IATP, STP, SRP, UTI, SMP, SM, PTP, FIRE, CRTP, CRUDP, SSCOPMCE, IPLT, SPS, PIPE, SCTP, FC, RSVP-E2E-IGNORE, Mobility-Header, UDPLite

protocolNumber Protocol, identified by protocol number, to match against the protocol of an incoming IPv6 packet. Minimum value: 1 Maximum value: 255

icmpType ICMP Message type to match against the message type of an incoming IPv6 ICMP packet. For example, to block DESTINATION UNREACHABLE messages, you must specify 3 as the ICMP type.

Note: This parameter can be specified only for the ICMP protocol. Minimum value: 0 Maximum value: 65536

icmpCode Code of a particular ICMP message type to match against the ICMP code of an incoming IPv6 ICMP packet. For example, to block DESTINATION HOST UNREACHABLE messages, specify 3 as the ICMP type and 1 as the ICMP code.

If you set this parameter, you must set the ICMP Type parameter. Minimum value: 0 Maximum value: 65536

vlan ID of the VLAN. The Citrix ADC applies the ACL6 rule only to the incoming packets on the specified VLAN. If you do not specify a VLAN ID, the appliance applies the ACL6 rule to the incoming packets on all VLANs. Minimum value: 1 Maximum value: 4094

vxlan ID of the VXLAN. The Citrix ADC applies the ACL6 rule only to the incoming packets on the specified VXLAN. If you do not specify a VXLAN ID, the appliance applies the ACL6 rule to the incoming packets on all VXLANs. Minimum value: 1 Maximum value: 16777215

interface ID of an interface. The Citrix ADC applies the ACL6 rule only to the incoming packets from the specified interface. If you do not specify any value, the appliance applies the ACL6 rule to the incoming packets from all interfaces.

priority Priority for the ACL6 rule, which determines the order in which it is evaluated relative to the other ACL6 rules. If you do not specify priorities while creating ACL6 rules, the ACL6 rules are evaluated in the order in which they are created. Minimum value: 1 Maximum value: 81920

logstate Enable or disable logging of events related to the ACL6 rule. The log messages are stored in the configured syslog or auditlog server.

Possible values: ENABLED, DISABLED Default value: DISABLED

ratelimit Maximum number of log messages to be generated per second. If you set this parameter, you must enable the Log State parameter. Default value: 100 Minimum value: 1 Maximum value: 10000

established Allow only incoming TCP packets that have the ACK or RST bit set if the action set for the ACL6 rule is ALLOW and these packets match the other conditions in the ACL6 rule.

dfdhash Specifies the type of hashmethod to be applied, to steer the packet to the FP of the packet.

Possible values: SIP-SPORT-DIP-DPORT, SIP, DIP, SIP-DIP, SIP-SPORT, DIP-DPORT

dfdprefix hashprefix to be applied to SIP/DIP to generate rsshash FP.eg 128 => hash calculated on the complete IP Default value: 128 Minimum value: 1 Maximum value: 128

stateful If stateful option is enabled, transparent sessions are created for the traffic hitting this ACL6 and not hitting any other features like LB, INAT etc.

Possible values: YES, NO Default value: NO

Example

set ns acl6 rule1 -srcPort 50

Related Commands

- apply ns acls6

rm ns acl6

Removes an ACL6 rule from the Citrix ADC. To commit this operation, you must apply the ACL6s.

Synopsis

rm ns acl6 <acl6name> ...

Arguments

acl6name Name of the ACL6 rule that you want to remove.

Example

rm ns acl6 rule1

Related Commands

- clear ns acls6

add ns acl6

Adds an ACL6 rule to the Citrix ADC. To commit this operation, you must apply the ACL6s. ACL6 rules filter data packets on the basis of various parameters, such as IP address, source port, action, and protocol.

Synopsis

add ns acl6 <acl6name> <acl6action> [-srcIPv6 <srcIPv6Val>] [-srcPort <srcPortVal>] [-destIPv6 <destIPv6Val>] [-destPort <destPortVal>] (-TTL <positive_integer> | -stateful (YES | NO)) [-srcMac <mac_addr>] [(-protocol <protocol>) | -protocolNumber <positive_integer>] [-icmpType <positive_integer>] [-type (CLASSIC | DFD)] [-logstate (ENABLED | DISABLED)]

Arguments

acl6name Name for the ACL6 rule. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

acl6action Action to perform on the incoming IPv6 packets that match the ACL6 rule. Available settings function as follows:

- ALLOW - The Citrix ADC processes the packet.
- BRIDGE - The Citrix ADC bridges the packet to the destination without processing it.
- DENY - The Citrix ADC drops the packet.

Possible values: BRIDGE, DENY, ALLOW

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

srcIPv6 IP address or range of IP addresses to match against the source IP address of an incoming IPv6 packet. In the command line interface, separate the range with a hyphen.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

srcIPv6Val Source IPv6 address (range).

srcPort Port number or range of port numbers to match against the source port number of an incoming IPv6 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

srcPortVal Source port (range). Maximum value: 65535

destIPv6 IP address or range of IP addresses to match against the destination IP address of an incoming IPv6 packet. In the command line interface, separate the range with a hyphen.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

destIPv6Val Destination IPv6 address (range).

destPort Port number or range of port numbers to match against the destination port number of an incoming IPv6 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

destPortVal Destination port (range). Maximum value: 65535

TTL Time to expire this ACL6 (in seconds). Minimum value: 1 Maximum value: 2147483647

srcMac MAC address to match against the source MAC address of an incoming IPv6 packet.

srcMacMask Used to define range of Source MAC address. It takes string of 0 and 1, 0s are for exact match and 1s for wildcard. For matching first 3 bytes of MAC address, srcMacMask value "000000111111". Default value: "000000000000"

protocol Protocol, identified by protocol name, to match against the protocol of an incoming IPv6 packet.

Possible values: ICMPV6, TCP, UDP, ICMP, IGMP, EGP, IGP, ARGUS, RDP, RSVP, EIGRP, L2TP, ISIS, GGP, IPoverIP, ST, CBT, BBN-RCC-M, NVP-II, PUP, EMCON, XNET, CHAOS, MUX, DCN-MEAS, HMP, PRM, XNS-IDP, TRUNK-1, TRUNK-2, LEAF-1, LEAF-2, IRTP, ISO-TP4, NETBLT, MFE-NSP, MERIT-INP, SEP, 3PC, IDPR, XTP, DDP, IDPR-CMTP, TP++, IL, IPv6, SDRP, IPv6-Route, IPv6-Frag, IDRP, GRE, MHRP, BNA, ESP, AH, I-NLSP, SWIPE, NARP, MOBILE, TLSP, SKIP, IPv6-NoNx, IPv6-Opts, Any-Host-Internal-Protocol, CFTP, Any-Local-Network, SAT-EXPAK, KRYPTOLAN, RVD, IPPC, Any-Distributed-File-System, TFTP, VISA, IPCV, CPNX, CPHB, WSN, PVP, BR-SAT-MO, SUN-ND, WB-MON, WB-EXPAK, ISO-IP, VMTP, SECURE-VM, VINES, TTP, NSFNET-IG, DGP, TCF, OSPFIGP, Sprite-RP, LARP, MTP, AX.25, IPIP, MICP, SCC-SP, ETHERIP, Any-Private-Encryption-Scheme, GMTP, IFMP, PNNI, PIM, ARIS, SCPS, QNX, A/N, IPComp, SNP, Compaq-Pe, IPX-in-IP, VRRP, PGM, Any-0-Hop-Protocol, ENCAP, DDX, IATP, STP, SRP, UTI, SMP, SM, PTP, FIRE, CRTP, CRUDP, SSCOPMCE, IPLT, SPS, PIPE, SCTP, FC, RSVP-E2E-IGNORE, Mobility-Header, UDPLite

protocolNumber Protocol, identified by protocol number, to match against the protocol of an incoming IPv6 packet. Minimum value: 1 Maximum value: 255

vlan ID of the VLAN. The Citrix ADC applies the ACL6 rule only to the incoming packets on the specified VLAN. If you do not specify a VLAN ID, the appliance applies the ACL6 rule to the incoming packets on all VLANs. Minimum value: 1 Maximum value: 4094

vxlan ID of the VXLAN. The Citrix ADC applies the ACL6 rule only to the incoming packets on the specified VXLAN. If you do not specify a VXLAN ID, the appliance applies the ACL6 rule to the incoming packets on all VXLANs. Minimum value: 1 Maximum value: 16777215

interface ID of an interface. The Citrix ADC applies the ACL6 rule only to the incoming packets from the specified interface. If you do not specify any value, the appliance applies the ACL6 rule to the incoming packets from all interfaces.

established Allow only incoming TCP packets that have the ACK or RST bit set if the action set for the ACL6 rule is ALLOW and these packets match the other conditions in the ACL6 rule.

icmpType ICMP Message type to match against the message type of an incoming IPv6 ICMP packet. For example, to block DESTINATION UNREACHABLE messages, you must specify 3 as the ICMP type.

Note: This parameter can be specified only for the ICMP protocol. Minimum value: 0 Maximum value: 65536

icmpCode Code of a particular ICMP message type to match against the ICMP code of an incoming IPv6 ICMP packet. For example, to block DESTINATION HOST UNREACHABLE messages, specify 3 as the ICMP type and 1 as the ICMP code.

If you set this parameter, you must set the ICMP Type parameter. Minimum value: 0 Maximum value: 65536

priority Priority for the ACL6 rule, which determines the order in which it is evaluated relative to the other ACL6 rules. If you do not specify priorities while creating ACL6 rules, the ACL6 rules are evaluated in the order in which they are created. Minimum value: 1 Maximum value: 81920

state State of the ACL6.

Possible values: ENABLED, DISABLED Default value: ENABLED

type Type of the acl6 ,default will be CLASSIC. Available options as follows:

- CLASSIC - specifies the regular extended acls.
- DFD - cluster specific acls,specifies hashmethod for steering of the packet in cluster .

Possible values: CLASSIC, DFD Default value: CLASSIC

dfdhash Specifies the type of hashmethod to be applied, to steer the packet to the FP of the packet.

Possible values: SIP-SPORT-DIP-DPORT, SIP, DIP, SIP-DIP, SIP-SPORT, DIP-DPORT

dfdprefix hashprefix to be applied to SIP/DIP to generate rsshash FP.eg 128 => hash calculated on the complete IP Default value: 128 Minimum value: 1 Maximum value: 128

stateful If stateful option is enabled, transparent sessions are created for the traffic hitting this ACL6 and not hitting any other features like LB, INAT etc.

Possible values: YES, NO Default value: NO

logstate Enable or disable logging of events related to the ACL6 rule. The log messages are stored in the configured syslog or auditlog server.

Possible values: ENABLED, DISABLED Default value: DISABLED

ratelimit Maximum number of log messages to be generated per second. If you set this parameter, you must enable the Log State parameter. Default value: 100 Minimum value: 1 Maximum value: 10000

Example

add ns acl6 rule1 DENY -srcport 45-1024 -destIPv6 2001::45 -protocol TCP

Related Commands

- apply ns acls6

disable ns acl6

Disables an ACL6 rule. To commit this operation, you must apply the ACL6s.After you apply the ACL6 rules, the Citrix ADC does not compare incoming IPv6 packets to the disabled ACL6 rules.

Synopsis

disable ns acl6 <acl6name> ...

Arguments

acl6name Name of ACL6 rule that you want to disable.

Example

disable ns acl6 rule1

Related Commands

- clear ns acls6

rename ns acl6

Renames an ACL6 rule. To commit this operation, you must apply the ACL6s.

Synopsis

rename ns acl6 <acl6name> <newName>

Arguments

acl6name Name of the ACL6 rule that you want to rename.

newName New name for the ACL6 rule. Must begin with an ASCII alphabetic or underscore \(_\) character, and must contain only ASCII alphanumeric, underscore, hash \(#\), period \(.\), space, colon \(:\), at \(@\), equals \(=\), and hyphen \(-\) characters.

Example

rename acl6 rule rule-new

unset ns acl6

Resets the attributes of the specified ACL6 rule. To commit this operation, you must apply the ACL6s.Attributes for which a default value is available revert to their default values. Refer to the set ns acl6 command for descriptions of the parameters..Refer to the set ns acl6 command for meanings of the arguments.

Synopsis

unset ns acl6 <acl6name>

Example

unset ns acl6 rule1 -srcPort

Related Commands

- apply ns acls6

ns-acls

The following operations can be performed on "ns-acls":

clear| renumber| apply|

clear ns acls

Removes all simple ACL rules from the Citrix ADC. This operation does not require an explicit apply.

Synopsis

clear ns acls

Arguments

type Type of the acl ,default will be CLASSIC. Available options as follows:

- CLASSIC - specifies the regular extended acls.
- DFD - cluster specific acls,specifies hashmethod for steering of the packet in cluster .

Possible values: CLASSIC, DFD Default value: CLASSIC

Example

clear ns acls -type <acltype>

renumber ns acls

Renumbers the priorities of extended ACL rules to multiples of 10. To commit this operation, you must apply the extended ACLs. Enables you to assign a new extended ACL rule a priority that is between two existing, consecutively numbered priorities. For example, if two extended ACLs, ACL1 and ACL2, have priorities 2 and 3 renumbering changes those priorities to 20 and 30. You can then add ACL3 with priority 25.

Synopsis

renumber ns acls

Arguments

type Type of the acl ,default will be CLASSIC. Available options as follows:

- CLASSIC - specifies the regular extended acls.
- DFD - cluster specific acls,specifies hashmethod for steering of the packet in cluster .

Possible values: CLASSIC, DFD Default value: CLASSIC

Example

renumber acls

apply ns acls

Updates the extended ACL rule's memory tree (lookup table), adding any new extended ACL rules and applying any modifications to existing ACL rules. The lookup table includes the configuration of all the extended ACL rules on the Citrix ADC. The Citrix ADC appliance uses the lookup table (not the configuration file) to filter the incoming IPv4 packets.

Synopsis

apply ns acls

Arguments

type Type of the acl ,default will be CLASSIC. Available options as follows:

- CLASSIC - specifies the regular extended acls.
- DFD - cluster specific acls,specifies hashmethod for steering of the packet in cluster .

Possible values: CLASSIC, DFD Default value: CLASSIC

Example

apply ns acls -type <acltype>

ns-acls6

The following operations can be performed on "ns-acls6":

apply| clear| renumber|

apply ns acls6

Updates the ACL6 rules' memory tree (lookup table), adding any new ACL6 rules and applying any modifications to existing ACL rules. The lookup table includes the configuration of all the ACL6 rules on the Citrix ADC. The Citrix ADC appliance uses the lookup table (not the configuration file) to filter the incoming IPv4 packets.

Synopsis

apply ns acls6

Arguments

type Type of the acl ,default will be CLASSIC. Available options as follows:

- CLASSIC - specifies the regular extended acls.
- DFD - cluster specific acls,specifies hashmethod for steering of the packet in cluster .

Possible values: CLASSIC, DFD Default value: CLASSIC

Example

apply ns acls6 -type <acltype>

Related Commands

- disable ns acl6

clear ns acls6

Removes all simple ACL6 rules from the Citrix ADC. This operation does not require an explicit apply.

Synopsis

clear ns acls6

Arguments

type Type of the acl ,default will be CLASSIC. Available options as follows:

- CLASSIC - specifies the regular extended acls.
- DFD - cluster specific acls,specifies hashmethod for steering of the packet in cluster .

Possible values: CLASSIC, DFD Default value: CLASSIC

Example

clear ns acls6 -type <acltype>

Related Commands

- rm ns acl6

renumber ns acls6

Renumbers the priorities of ACL6 rules to multiples of 10. To commit this operation, you must apply the ACL6s. Enables you to assign a new ACL6 rule a priority that is between two existing, consecutively numbered priorities. For example, if two ACL6s, ACL6-1 and ACL6-2, have priorities 2 and 3 renumbering changes those priorities to 20 and 30. You can then add ACL6-3 with priority 25.

Synopsis

renumber ns acls6

Arguments

type Type of the acl ,default will be CLASSIC. Available options as follows:

- CLASSIC - specifies the regular extended acls.
- DFD - cluster specific acls,specifies hashmethod for steering of the packet in cluster .

Possible values: CLASSIC, DFD Default value: CLASSIC

Example

renumber acls6

ns-appflowCollector

The following operations can be performed on "ns-appflowCollector":

show| rm| add|

show ns appflowCollector

Display details of all the AppFlow collectors configured on the system. Alternatively, to view the details of a particular AppFlow collector, specify its name. NOTE: This command is deprecated.This command is deprecated in favor of 'show appflow collector'

Synopsis

Arguments

name Name of the AppFlow collector.

Output

IPAddress The IPv4 address of the AppFlow collector.

port The UDP port on which the AppFlow collector is listening.

devno count stateflag

Example

show ns appflowCollector collector1

rm ns appflowCollector

Remove an AppFlow collector. NOTE: This command is deprecated.This command is deprecated in favor of 'rm appflow collector'

Synopsis

Arguments

name Name of an AppFlow collector.

Example

rm ns appflowCollector collector1

add ns appflowCollector

Add a new AppFlow collector. NOTE: This command is deprecated.This command is deprecated in favor of 'add appflow collector'

Synopsis

Arguments

name Name of the AppFlow collector.

IPAddress The IPv4 address of the AppFlow collector.

port The UDP port on which the AppFlow collector is listening. Default value: 4739

Example

add ns appflowCollector collector1 -IPAddress 192.168.1.40 -port 2055

ns-appflowParam

The following operations can be performed on "ns-appflowParam":

set| unset| show|

set ns appflowParam

Set AppFlow parameters. NOTE: This command is deprecated.

Synopsis

Arguments

templateRefresh IPFIX template refresh interval (in seconds). Default value: 600 Minimum value: 60 Maximum value: 3600

udpPmtu MTU to be used for IPFIX UDP packets. Default value: 1472 Minimum value: 128 Maximum value: 1472

httpUrl Enable AppFlow HTTP URL logging.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpCookie Enable AppFlow HTTP cookie logging.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpReferer Enable AppFlow HTTP referer logging.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpMethod Enable AppFlow HTTP method logging.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpHost Enable AppFlow HTTP host logging.

Possible values: ENABLED, DISABLED Default value: DISABLED

httpUserAgent Enable AppFlow HTTP user-agent logging.

Possible values: ENABLED, DISABLED Default value: DISABLED

clientTrafficOnly Control whether AppFlow records should be generated only for client-side traffic.

Possible values: YES, NO Default value: NO

Example

set ns appflowParam -templateRefresh 240

unset ns appflowParam

Use this command to remove ns appflowParam settings.Refer to the set ns appflowParam command for meanings of the arguments.NOTE: This command is deprecated.

Synopsis

show ns appflowParam

Display AppFlow parameters. NOTE: This command is deprecated.This command is deprecated in favor of 'show appflow param'

Synopsis

Arguments

Output

templateRefresh IPFIX template refresh interval (in seconds).

udpPmtu MTU to be used for IPFIX UDP packets.

httpUrl Enable AppFlow HTTP URL logging.

httpCookie Enable AppFlow HTTP cookie logging.

httpReferer Enable AppFlow HTTP referer logging.

httpMethod Enable AppFlow HTTP method logging.

httpHost Enable AppFlow HTTP host logging.

httpUserAgent Enable AppFlow HTTP user-agent logging.

clientTrafficOnly Control whether AppFlow records should be generated only for client-side traffic.

ns-aptlicense

The following operations can be performed on "ns-aptlicense":

show| update|

show ns aptlicense

Synopsis

show ns aptlicense <serialNo>

Arguments

serialNo Hardware Serial Number/License Activation Code(LAC)

useProxy Specifies whether to use the licenseproxyserver to reach the internet. Make sure to configure licenseproxyserver to use this option.

Possible values: YES, NO Default value: NO

Output

response Response data as text blob

id License ID

sessionId Session ID

bindType Bind type

countAvailable Count

countTotal Count

name License name

relevance License relevance

datePurchased License purchase date

dateSa License SA date

dateExp License expiry date

features Features

Example

show ns aptlicense <hw-no/lac>

update ns aptlicense

Synopsis

update ns aptlicense <id> <sessionId> <bindType> <countAvailable>

Arguments

id License ID

sessionId Session ID

bindType Bind type

countAvailable The user can allocate one or more licenses. Ensure the value is less than (for partial allocation) or equal to the total number of available licenses

licenseDir License Directory

useProxy Specifies whether to use the licenseproxyserver to reach the internet. Make sure to configure licenseproxyserver to use this option.

Possible values: YES, NO Default value: NO

Example

update ns aptlicense key1 sessionID# HOSTNAME 1

ns-assignment

The following operations can be performed on "ns-assignment":

rm| show| rename| set| unset| add|

rm ns assignment

Removes a rewrite action.

Synopsis

rm ns assignment <name>

Arguments

name Name for the assignment. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the assignment is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my assignment" or my assignment).

Example

rm ns assignment set_user_privilege

show ns assignment

Displays configured assignements.

Synopsis

show ns assignment

Arguments

name Name of the assignment

Output

stateflag variable Left hand side of the assignment.

set Right hand side of the assignment, variable set to expression value.

add Right hand side of the assignment, expression value added to variable.

sub Right hand side of the assignment, expression value subtracted from variable.

append Right hand side of the assignment, expression value appended to vari able.

clear Variable cleared.

hits The number of times the action has been taken.

undefHits The number of times the action resulted in UNDEF.

referenceCount The number of references to the action.

comment Comment. Can be used to preserve information about this rewrite action.

devno count

Example

show ns assignment

rename ns assignment

Renames an assignment.

Synopsis

rename ns assignment <name>@ <newName>@

Arguments

name Existing name of the assignment.

newName New name for the assignment. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#),

space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the rewrite policy is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my assignment" or my assignment).

Example

rename ns assignment oldname newname

set ns assignment

Sets an assignment of a value to a variable.

Synopsis

set ns assignment <name>

Arguments

name Name for the assignment. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the assignment is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my assignment" or my assignment).

variable Left hand side of the assigment, of the form $variable-name (for a singleton variabled) or $variable-name, where key-expression is an expression that evaluates to a text string and provides the key to select a map entry

set Right hand side of the assignment. The expression is evaluated and assigned to the left hand variable.

add Right hand side of the assignment. The expression is evaluated and added to the left hand variable.

sub Right hand side of the assignment. The expression is evaluated and subtracted from the left hand variable.

append Right hand side of the assignment. The expression is evaluated and appended to the left hand variable.

clear Clear the variable value. Deallocates a text value, and for a map, the text key.

comment Comment. Can be used to preserve information about this rewrite action.

Example

set ns assignment set_user_privilege -var $user_privilege_map -set sys.http.callout(get_user_privilege)

unset ns assignment

Use this command to remove ns assignment settings.Refer to the set ns assignment command for meanings of the arguments.

Synopsis

unset ns assignment <name> -comment

add ns assignment

Creates an assignment of a value to a variable. The variable (the left hand side) may be a singleton variable or a map with a key expression. The value (the right hand side) is computed from an expression and may be used to set the variable or may be added to or subtracted from the current value of a ulong variable or appended to a text variable. The key expression, if present, is evaluated before the value expression. The left hand side variable value may also be cleared, in which case there is no value expression.

Synopsis

add ns assignment <name> -variable <expression>

Arguments

name Name for the assignment. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the assignment is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my assignment" or my assignment).

variable Left hand side of the assigment, of the form $variable-name (for a singleton variabled) or $variable-name, where key-expression is an expression that evaluates to a text string and provides the key to select a map entry

set Right hand side of the assignment. The expression is evaluated and assigned to the left hand variable.

add Right hand side of the assignment. The expression is evaluated and added to the left hand variable.

sub Right hand side of the assignment. The expression is evaluated and subtracted from the left hand variable.

append Right hand side of the assignment. The expression is evaluated and appended to the left hand variable.

clear Clear the variable value. Deallocates a text value, and for a map, the text key.

comment Comment. Can be used to preserve information about this rewrite action.

Example

add ns assignment set_user_privilege -var $user_privilege_map -set sys.http.callout(get_user_privilege)

ns-capacity

The following operations can be performed on "ns-capacity":

show| unset| set|

show ns capacity

Displays the running capacity of the system.

Synopsis

show ns capacity

Arguments

Output

actualbandwidth Bandwith in MBPS.

platform appliance platform type.

vcpuCount number of vCPUs licensed.

maxVcpuCount number of max vCPUs.

Edition Product edition Standard/Enterprise/Platinum.

unit Bandwidth unit GBPS/MBPS.

bandwidth Configured Bandwidth.

maxbandwidth Maximum Bandwidth.

minbandwidth Minimum Bandwidth.

instancecount VPX will consume one instance and MPX will consume zero instance

unset ns capacity

Use this command to undo configuration changes made to ns capacity parameters..Refer to the set ns capacity command for meanings of the arguments.

Synopsis

unset ns capacity (-bandwidth | -platform | -vcpu)

set ns capacity

Modifies the system capacity. Capacity will be check-out from the license pool of License Server

Synopsis

set ns capacity ((-bandwidth <positive_integer> -unit (Gbps | Mbps)) | -platform <platform> | -Edition <Edition> | -vcpu)

Arguments

bandwidth System bandwidth limit. Minimum value: 0

platform appliance platform type.

Possible values: VS10, VE10, VP10, VS25, VE25, VP25, VS50, VE50, VP50, VS200, VE200, VP200, VS1000, VE1000, VP1000, VS3000, VE3000, VP3000, VS5000, VE5000, VP5000, VS8000, VE8000, VP8000, VS10000, VE10000, VP10000, VS15000, VE15000, VP15000, VS25000, VE25000, VP25000, VS40000, VE40000, VP40000, VS100000, VE100000, VP100000, CP1000

vcpu licensed using vcpu pool.

Edition Product edition.

Possible values: Standard, Enterprise, Platinum

unit Bandwidth unit.

Possible values: Gbps, Mbps

ns-centralmanagementserver

The following operations can be performed on "ns-centralmanagementserver":

rm| add| show|

rm ns centralmanagementserver

Removes a central management server profile and the associated configuration.

Synopsis

rm ns centralmanagementserver <type>

Arguments

type Type of the centralmgmtserver user to remove.

Possible values: CLOUD, ONPREM

add ns centralmanagementserver

Adds a centralmgmtserver server profile and verifies the configuration to ensure that it is correct. Also registers the device on the central management server.

Synopsis

add ns centralmanagementserver <type> (-IPAddress <ip_addr|ipv6_addr|*> | -serverName <string>)

Arguments

type Type of the central management server. Must be either CLOUD or ONPREM depending on whether the server is on the cloud or on premise.

Possible values: CLOUD, ONPREM

userName Username for access to central management server. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my ns centralmgmtserver" or "my ns centralmgmtserver").

password Password for access to central management server. Required for any user account.

activationCode Activation code is used to register to ADM service

IPAddress Ip Address of central management server.

serverName Fully qualified domain name of the central management server or service-url to locate ADM service.

validateCert validate the server certificate for secure SSL connections.

Possible values: YES, NO Default value: YES

deviceProfileName Device profile is created on ADM and contains the user name and password of the instance(s).

adcUserName ADC username used to create device profile on ADM

adcPassword ADC password used to create device profile on ADM

Example

add ns centralmgmtserver cloud johndoe abcd The above example adds user johndoe with password abcd

show ns centralmanagementserver

Displays the current configuration of a central management server profile.

Synopsis

show ns centralmanagementserver

Arguments

type Type of the central management server profile.

Possible values: CLOUD, ONPREM

Output

userName Username for access to the central management server.

IPAddress Ip Address of central management server.

serverName Fully qualified domain name of the central management server.

validateCert validate the server certificate for secure SSL connections.

password Password for access to the central management server.

deviceProfileName Device profile is created on ADM and contains the user name and password of the instance(s).

InstanceID Instance ID of the customer provided by Trust

CustomerID Customer ID of the citrix cloud customer

ADMServiceEnvironment ADM service environment (PRODUCTION/STAGING/DEV)

ADMServiceConnectionStatus Built-in agent's (mastools) connection status to ADM service

devno count stateflag

Example

Example

```
show ns centralmgmtserver ONPREM Type: ONPREM UserName: joe IPAddress:
10.102.1.123 Password:
b04b0ac4e363c4b05d9a3e84cfbfd75763d11c5546ca7d4abb133a249ea8440e Done
```

Ns

The entities on which you can perform NetScaler CLI operations:

- ns-acl
- ns-acl6
- ns-acls
- ns-acls6
- ns-appflowCollector

- ns-appflowParam
- ns-aptlicense
- ns-assignment
- ns-capacity
- ns-centralmanagementserver
- ns-config
- ns-connectiontable
- ns-consoleloginprompt
- ns-cqaparam
- ns-dhcpIp
- ns-dhcpParams
- ns-diameter
- ns-encryptionKey
- ns-encryptionParams
- ns-events
- ns-extension
- ns-feature
- ns-hardware
- ns-hmacKey
- ns-hostName
- ns-httpParam
- ns-httpProfile
- ns-icapProfile
- ns-idletimeout
- ns-info
- ns-ip
- ns-ip6
- ns-job
- ns-license
- ns-licenseparameters

- ns-licenseproxyserver
- ns-licenseserver
- ns-licenseserverpool
- ns-limitIdentifier
- ns-limitSelector
- ns-limitSessions
- ns-memory
- ns-memrecovery
- ns-migration
- ns-mode
- ns
- ns-ns.conf
- ns-param
- ns-partition
- ns-partitionMAC
- ns-pbr
- ns-pbr6
- ns-pbrs
- ns-rateControl
- reboot
- ns-rollbackcmd
- ns-rpcNode
- ns-runningConfig
- ns-savedConfig
- ns-serviceFunction
- ns-servicePath
- shutdown
- ns-simpleacl
- ns-simpleacl6
- ns-sourceroutecachetable

- ns-spParams
- ns-stats
- ns-surgeQ
- ns-tcpParam
- ns-tcpProfile
- ns-tcpbufParam
- ns-testlicense
- ns-timeout
- ns-timer
- ns-timezone
- ns-trafficDomain
- ns-variable
- ns-version
- ns-vpxparam
- ns-weblogparam
- ns-xmlnamespace

ns-config

The following operations can be performed on "ns-config":

set| unset| show| clear| query| save| diff|

set ns config

Sets the Citrix ADC IP address and Citrix ADC VLAN. To set other Citrix ADC parameters, use the 'set ns param' command. Note: To change the NSIP address or the NSVLAN of an appliance that is part of a cluster, first remove the appliance from the cluster, change the NSIP or the NSVLAN, and then add the appliance back to the cluster.

Synopsis

set ns config [-nsvlan <positive_integer> -ifnum <interface_name> ...]

Arguments

IPAddress IP address of the Citrix ADC. Commonly referred to as NSIP address. This parameter is mandatory to bring up the appliance.

netmask Netmask corresponding to the IP address. This parameter is mandatory to bring up the appliance.

nsvlan VLAN (NSVLAN) for the subnet on which the IP address resides. Minimum value: 2 Maximum value: 4094

ifnum Interfaces of the appliances that must be bound to the NSVLAN. Minimum value: 1

tagged Specifies that the interfaces will be added as 802.1q tagged interfaces. Packets sent on these interface on this VLAN will have an additional 4-byte 802.1q tag which identifies the VLAN. To use 802.1q tagging, the switch connected to the appliance's interfaces must also be configured for tagging.

Possible values: YES, NO Default value: YES

unset ns config

Removes the attributes of the Citrix ADC. Attributes for which a default value is available revert to their default values. Refer to the 'set ns config' command for a description of the parameters..Refer to the set ns config command for meanings of the arguments.

Synopsis

unset ns config

show ns config

Displays the following details of the Citrix ADC:

- Citrix ADC IP address and subnet mask
- Number of mapped IP addresses
- Identifies the appliance as a standalone appliance, a part of a HA pair, or is a cluster node
- Current time on the system and timestamp when the appliance was last updated Note: To view the complete configurations that have been executed on the appliance, run the 'show ns runningConfig' command.

Synopsis

show ns config

Arguments

Output

IPAddress IP Address of the System.

netmask The netmask corresponding to the IP address.

mappedIP Mapped IP Address of the System.

range The range of Mapped IP addresses to be configured.

nsvlan The VLAN (NSVLAN) for the subnet on which the system IP resides.

ifnum Bind the given ports to the NSVLAN.

tagged Specifies that the interfaces will be added as 802.1q tagged interfaces. Packets sent on these interface on this VLAN will have an additional 4-byte 802.1q tag which identifies the VLAN. To use 802.1q tagging, the switch connected to the appliance's interfaces must also be configured for tagging.

svmCmd Identifies the source of command. When SVM fires the nitro command, it will set the value of SVMCMD to be 1 and in other cases it will be 0.

httpPort The HTTP ports on the Web server.

maxConn Maximum Number of Connections.

maxReq Maxmimum Number of requests that can be handled.

cip Insertion of client IP address into the HTTP header.

cipHeader The text that will be used as the client IP header.

cookieversion The version of the cookie inserted by system.

secureCookie enable/disable secure flag for persistence cookie

failover Standalone node.

systemType The type of the System. Possible Values: Standalone, HA, Cluster

primaryIP HA Master Node IP address.

primaryIP6 pmtuMin The minimum Path MTU.

pmtuTimeout The timeout value in minutes.

ftpPortRange Port range configured for FTP services.

crPortRange Port range for cache redirection services.

flags The flags for this entry.

timezone Name of the timezone

LastConfigChangedTime Time when the configuration was last modified.

LastConfigSaveTime Time when the configuration was last saved through savensconfig.

currentSytemTime current system time in date format.

systemTime current system time.

grantQuotaMaxClient The percentage of shared quota to be granted at a time for maxClient

exclusiveQuotaMaxClient The percentage of maxClient to be given to PEs

grantQuotaSpillOver The percentage of shared quota to be granted at a time for spillover

exclusiveQuotaSpillOver The percentage of max limit to be given to PEs

nwfwmode Network Firewallmode

ConfigChanged returns True if configuration has changed since last saved config.

clear ns config

Clears the Citrix ADC running configurations based on different levels.

Synopsis

clear ns config <level>

Arguments

force Configurations will be cleared without prompting for confirmation.

level Types of configurations to be cleared.

- basic: Clears all configurations except the following:
- NSIP, default route (gateway), static routes, MIPs, and SNIPs
- Network settings (DG, VLAN, RHI and DNS settings)
- Cluster settings
- HA node definitions
- Feature and mode settings
- nsroot password
- extended: Clears the same configurations as the 'basic' option. In addition, it clears the feature and mode settings.
- full: Clears all configurations except NSIP, default route, and interface settings. Note: When you clear the configurations through the cluster IP address, by specifying the level as 'full', the cluster is deleted and all cluster nodes become standalone appliances. The 'basic' and 'extended' levels are propagated to the cluster nodes.

Possible values: basic, extended, full

RBAconfig RBA configurations and TACACS policies bound to system global will not be cleared if RBA is set to NO.This option is applicable only for BASIC level of clear configuration.Default is YES, which will clear rba configurations.

Possible values: YES, NO Default value: YES

query ns config

Queries NS config

Synopsis

query ns config

Arguments

weakpassword Option to list all weak passwords (not adhering to strong password requirements). Takes config file as input, if no input specified, running configuration is considered. Command => query ns config -weakpassword / query ns config -weakpassword /nsconfig/ns.conf

changedpassword Option to list all passwords changed which would not work when downgraded to older releases. Takes config file as input, if no input specified, running configuration is

considered. Command => query ns config -changedpassword / query ns config -changedpassword /nsconfig/ns.conf

config configuration File to be used to find weak passwords, if not specified, running config is taken as input.

Output

response

Example

query ns config -weakpassword query ns config -changedpassword query ns config -weakpassword -config <config file full path> query ns config -changedpassword -config <config file full path>

save ns config

Save the configurations to the appliances FLASH memory in the /nsconfig/ns.conf file. Backup configuration files are named ns.conf.n. The most recent backup file has the smallest value for n.

Synopsis

save ns config

Arguments

all Use this option to do saveconfig for all partitions

Output

message

diff ns config

Difference between two configuration

Synopsis

diff ns config

Arguments

config1 Location of the configurations.

config2 Location of the configurations.

outtype Format to display the difference in configurations.

Possible values: cli, xml

template File that contains the commands to be compared.

ignoreDeviceSpecific Suppress device specific differences.

Output

response

Example

Generates the differences between two configurations. Note: If no parameters are provided, then the differences between the saved configurations and the running configurations are shown.

ns-connectiontable

The following operations can be performed on "ns-connectiontable":

show ns connectiontable

Displays the current TCP/IP connection table.

Synopsis

show ns connectiontable

Arguments

filterexpression The maximum length of filter expression is 255 and it can be of following format: <expression>

```
&lt;relop> = ( && | || )



&lt;expression> =:

CONNECTION.&lt;qualifier>.&lt;qualifier-method>.(&lt;qualifier-value>)



&lt;qualifier> = SRCIP
```

```
&lt;qualifier-method> = [ EQ | NE ]

&lt;qualifier-value>  = A valid IPv4 address

example = CONNECTION.SRCIP.EQ(127.0.0.1)



&lt;qualifier> = DSTIP

&lt;qualifier-method> = [ EQ | NE ]

&lt;qualifier-value>  = A valid IPv4 address.

example = CONNECTION.DSTIP.EQ(127.0.0.1)



&lt;qualifier> = IP

&lt;qualifier-method> = [ EQ | NE ]

&lt;qualifier-value>  = A valid IPv4 address.

example = CONNECTION.IP.EQ(127.0.0.1)



&lt;qualifier> = SRCIPv6

&lt;qualifier-method> = [ EQ | NE ]

&lt;qualifier-value>  = A valid IPv6 address.

example = CONNECTION.SRCIPv6.EQ(2001:db8:0:0:1::1)



&lt;qualifier> = DSTIPv6

&lt;qualifier-method> = [ EQ | NE ]

&lt;qualifier-value>  = A valid IPv6 address.
```

```
example = CONNECTION.DSTIPv6.EQ(2001:db8:0:0:1::1)



&lt;qualifier> = IPv6

&lt;qualifier-method> = [ EQ | NE ]

&lt;qualifier-value>  = A valid IPv6 address.

example = CONNECTION.IPv6.EQ(2001:db8:0:0:1::1)



&lt;qualifier> = SRCPORT

&lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE

                    | BETWEEN ]

&lt;qualifier-value>  = A valid port number.

example = CONNECTION.SRCPORT.EQ(80)



&lt;qualifier> = DSTPORT

&lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE

                    | BETWEEN ]

&lt;qualifier-value>  = A valid port number.

example = CONNECTION.DSTPORT.EQ(80)



&lt;qualifier> = PORT

&lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE

                    | BETWEEN ]
```

```
&lt;qualifier-value>  = A valid port number.

example = CONNECTION.PORT.EQ(80)



&lt;qualifier> = SVCNAME

&lt;qualifier-method> = [ EQ | NE | CONTAINS | STARTSWITH

                    | ENDSWITH ]

&lt;qualifier-value>  = service name.

example = CONNECTION.SVCNAME.EQ("name")



&lt;qualifier> = LB_VSERVER.NAME

&lt;qualifier-method> = [ EQ | NE | CONTAINS | STARTSWITH

                    | ENDSWITH ]

&lt;qualifier-value>  = LB vserver name.

example = CONNECTION.LB_VSERVER.NAME.EQ("name")



&lt;qualifier> = CS_VSERVER.NAME

&lt;qualifier-method> = [ EQ | NE | CONTAINS | STARTSWITH

                    | ENDSWITH ]

&lt;qualifier-value>  = CS vserver name.

example = CONNECTION.CS_VSERVER.NAME.EQ("name")



&lt;qualifier> = INTF
```

```
&lt;qualifier-method> = [ EQ | NE ]

&lt;qualifier-value>  = A valid interface id in the form of

            x/y (n/x/y in case of cluster interface).

examle = CONNECTION.INTF.EQ("0/1/1")



&lt;qualifier> = VLANID

&lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE

                    | BETWEEN ]

&lt;qualifier-value>  = A valid VLAN ID.

example = CONNECTION.VLANID.EQ(0)



&lt;qualifier> = CONNID

&lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE

                    | BETWEEN ]

&lt;qualifier-value>  = A valid PCB dev number.

example = CONNECTION.CONNID.EQ(0)



&lt;qualifier> = PPEID

&lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE

                    | BETWEEN ]

&lt;qualifier-value>  = A valid core ID.

  example = CONNECTION.PPEID.EQ(0)
```

```
&lt;qualifier> = IDLETIME

&lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE

                    | BETWEEN ]

&lt;qualifier-value>  = A positive integer indicating the

               idletime.

example = CONNECTION.IDLETIME.LT(100)



&lt;qualifier> = TCPSTATE

&lt;qualifier-method> = [ EQ | NE ]

&lt;qualifier-value>  = ( CLOSE_WAIT | CLOSED | CLOSING |

       ESTABLISHED | FIN_WAIT_1 | FIN_WAIT_2 | LAST_ACK |

    LISTEN | SYN_RECEIVED | SYN_SENT | TIME_WAIT |

    NOT_APPLICABLE)

example = CONNECTION.TCPSTATE.EQ(LISTEN)



&lt;qualifier> = SERVICE_TYPE

&lt;qualifier-method> = [ EQ | NE ]

&lt;qualifier-value>  = ( SVC_HTTP | FTP | TCP | UDP | SSL |

    SSL_BRIDGE | SSL_TCP | NNTP | RPCSVR | RPCSVRS |

    RPCCLNT | SVC_DNS | ADNS | SNMP | RTSP | DHCPRA | NAT | ANY |

    MONITOR | MONITOR_UDP | MONITOR_PING | SIP_UDP |
```

```
    SVC_MYSQL | SVC_MSSQL | SERVICE_UNKNOWN )
example = CONNECTION.SERVICE_TYPE.EQ(ANY)


&lt;qualifier> = TRAFFIC_DOMAIN_ID
&lt;qualifier-method> = [ EQ | NE | GT | GE | LT | LE
                    | BETWEEN ]
&lt;qualifier-value>  = A valid traffic domain ID.
example = CONNECTION.TRAFFIC_DOMAIN_ID.EQ(0)


common usecases:
Filtering out loopback connections and view present


connections through netscaler
show connectiontable "CONNECTION.IP.NE(127.0.0.1) &&
CONNECTION.TCPSTATE.EQ(ESTABLISHED)" -detail full


show connections from a particular sourceip and targeted
to port 80
show connectiontable "CONNECTION.SRCIP.EQ(10.102.1.91) &&
CONNECTION.DSTPORT.EQ(80)"


show connection particular to a service and its linked
```

```
client connections

show connectiontable CONNECTION.SVCNAME.EQ("S1")

-detail link



show connections for a particular servicetype(e.g.http)

show connectiontable CONNECTION.SERVICE_TYPE.EQ(TCP)



viewing connections that have been idle for a long time

show connectiontable CONNECTION.IDLETIME.GT(100)



show connections particular to a service and idle

for a long time

show connectiontable "CONNECTION.SVCNAME.EQ(\\"S1\\") &&

CONNECTION.IDLETIME.GT(100)"



show connections for a particular interface

show connectiontable CONNECTION.INTF.EQ("1/1")



show connections for a particular interface and vlan

show connectiontable "CONNECTION.INTF.EQ(\\"1/1\\") &&

CONNECTION.VLANID.EQ(1)"
```

detail Specify display options for the connection table.

- LINK - Displays the linked PCB (Protocol Control Block).
- NAME - Displays along with the service name.
- CONNFAILOVER - Displays PCB with connection failover.
- FULL - Displays all available details.

Listen Display listening services only

Output

SOURCEIP Source IP of the connection.

SOURCEPORT Source port of the connection.

DESTIP Destination IP of the connection.

DESTPORT Destination port of the connection.

SVCTYPE Protocol supported by the connection.

IDLETIME Time since last activity was detected on the connection.

STATE Current TCP/IP state of the connection.

linkSourceIP Source IP of the link connection.

linkSourcePort Source port of the link connection.

linkDestIP Destination IP of the link connection.

linkDestPort Destination port of the link connection.

linkServiceType Protocol supported by the link connection.

linkIdleTime Time since last activity was detected on link connection.

linkState TCP/IP current state of link connection.

entityName Citrix ADC entity name for the connection.

linkEntityName Citrix ADC entity name for link connection.

connectionNumber Connection number

linkConnectionNumber Link connection number

connid Unique transaction number for the connection.

linkConnid Unique transaction number for the peer connection.

connProperties flags used to store connection properties like client, server etc.

optionFlags flags used to store TCP options like Sack, WS

nsWSvalue Citrix ADC window scaling value

peerWSvalue peer window scaling value

mss Client side MSS for the connection - used in server SYN.

retxRetryCnt Retransmission retry count for the connection.

rcvWnd Received Advertised Window for the connection.

advWnd Sent advertised window for the connection.

sndCwnd sent congestion window for the connection.

iss Initial send sequence number for the connection.

irs Initial receive sequence number for the connection.

rcvNxt next expecting seq number for the connection.

maxAck current running max ack sent for the connection.

sndNxt next bytes seq number for the connection.

sndUnAck Most recently received ACK for the connection.

httpEndSeq HTTP parsing tracking seq number for the connection.

httpState HTTP Protocol state for the connection.

trCount Max reuests allowed per connection.

priority priority of the connection.

httpReqVer current HTTP request version on the connection.

httpRequest current HTTP request type on the connection.

httpRspCode current response type on the connection.

rttSmoothed smoothed RTT value of the connection.

rttVariance RTT variance for the connection.

outoforderPkts held packets on the connection.

count count

linkOptionFlag Link connection's TCP option flag for Sack and WS

linknsWSvalue Link connection-s Citrix ADC window scaling value

linkpeerWSvalue Link connection-s peer Citrix ADC window scaling value

linkMSS Client side MSS for the Link connection - used in server SYN

linkRetxRetryCnt Retransmission retry count for the Link connection.

linkRcvWnd Received Advertised Window for the Link connection.

linkAdvWnd Sent advertised window for the Link connection.

linkSndCwnd Send congestion window for the Link connection.

linkISS Initial send seq number for the Link connection.

linkIRS Initial receive seq number for the Link connection.

linkRcvNxt Next expecting seq number on the Link connection.

linkMaxAck Current running maximum ack sent on the Link connection.

linkSndNxt Next bytes seq number for the Link connection.

linkSndUnAck Most recently received ACK on the Link connection.

linkHttpEndSeq HTTP parsing tracking seq number on the Link connection.

linkHttpState HTTP protocol state on the Link connection.

linkTrCount Max requests per connection for Link connection.

linkPriority Priority for the Link connection.

linkHttpReqVer HTTP current request version on Link connection.

linkHttpReq HTTP current request type on Link connection.

linkHttpRspCode Current response type on link connection.

linkRttSmoothed Smoothed RTT value on link connection.

linkRttVariance RTT variance on Link connection.

linkHeldPkts Held packets on Link connection.

targetnodeidnnm NNM connection target node ID.

sourcenodeidnnm NNM connection source node ID.

channelidnnm NNM connection channel ID.

msgversionnnm nnm message version.

td Traffic Domain Id.

maxRcvbuf Maximum receive window that application advertizes to peer.

linkmaxRcvbuf Maximum receive window that application advertizes to peer in linked connection.

RxQsize Total number of bytes in Citrix ADC receive buffer. This includes bytes being processed / policy related data / stored in application buffer.

linkRxQsize Total number of bytes in Citrix ADC receive buffer for linked connection. This includes bytes being processed / policy related data / stored in application buffer.

maxSndbuf Maximum send window that application can process and send.

linkmaxSndbuf Maximum send window that application can process and send in linked connection.

TxQsize Total number of bytes in Citrix ADC send buffer. This includes both inflight and queued bytes in Citrix ADC.

linkTxQsize Total number of bytes in Citrix ADC send buffer for linked connection. This includes both inflight and queued bytes in Citrix ADC.

flavor TCP congestion control algorithm.

linkflavor TCP congestion control algorithm for a linked connection.

bwEstimate TCP Bandwidth Estimate

linkbwEstimate TCP Bandwidth Estimate for a linked connection

rttMin Minimum Round Trip Time for the connection.

linkrttMin Minimum Round Trip Time for linked connection.

name Name of TCP profile attached to the connection.

linkName Name of TCP profile attached to the connection.

tcpmode TCP Optimization modes TRANSPARENT / ENDPOINT.

linktcpmode TCP Optimization modes TRANSPARENT / ENDPOINT for linked connection.

realTimeRtt Real Time / Instantaneous round trip time.

linkrealTimeRtt Real Time / Instantaneous round trip time for linked connection.

sndBuf send buffer size.

linksndBuf Send buffer size for linked connection.

nsbTcpwaitQ Number of packets in TCP wait queue.

linknsbTcpwaitQ Number of packets in wait queue for linked connection.

nsbRetxQ Number of packets in retransmission queue.

linknsbRetxQ Number of packets in retransmission queue for linked connection.

sackblocks Number of sack blocks attached to the connection.

linksackblocks Number of sack blocks attached in linked connection.

congstate TCP congestion state.

linkcongstate TCP congestion state for a linked connection.

sndrecoverle Sequence Number denoting end of fast recovery.

linksndrecoverle Sequence Number denoting end of fast recovery for linked connection.

creditsInBytes Connections current credits in Bytes/ms.

linkcredits Link connections current credits in Bytes/ms.

rateInBytes Connections current rate in Bytes/ms

linkrateInBytes Link connections current rate in Bytes/ms

rateSchedulerQueue Bytes that are queued in the rate scheduler for this connection

linkrateSchedulerQueue Bytes that are queued in the rate scheduler for link connection

burstRateControl TCP Burst Rate Control DISABLED/FIXED/DYNAMIC.

linkburstRateControl TCP Burst Rate Control DISABLED/FIXED/DYNAMIC.

cqaBifAvg Average bytes in flight over maxburst.

cqaThruputAvg Average instantaneous throughput over maxburst.

cqaRcvwndAvg Average receive window over maxburst.

cqaIai1msPct Percentage of inter arriaval samples for 1ms over maxburst.

cqaIai2msPct Percentage of inter arriaval samples for 2ms over maxburst.

cqaSamples Number of ACK samples over maxburst.

cqaIaiSamples Number of samples considered for calculating inter arrival interval over maxburst.

cqaNetClass Network type name.

cqaCCL Connection congestion level

cqaCSQ Connectiontion signal quality level

cqaIaiAvg Average inter arriaval interval over maxburst

cqaIsiAvg Average inter send interval over maxburst

cqaRcvwndMin Minimum receive window over maxburst

cqaRetxCorr Number of retransmission due to noise over maxburst

cqaRetxCong Number of retransmission due to congestion over maxburst

cqaRetxPackets Number of retransmission over maxburst

cqaLoadDelayAvg Average load delay over maxburst

cqaNoiseDelayAvg Average noise delay over maxburst

cqaRttMax Maximum RTT sample over maxburst in ms

cqaRttMin Minimum RTT sample over maxburst in ms

cqaRttAvg Minimum RTT sample over maxburst in ms

adaptiveTcpProfName Name of the Adaptive-TCP profile currently assigned to the connection.

outoforderBlocks held packets on the connection.

outoforderFlushedCount held packets on the connection.

outoforderBytes held packets on the connection.

devno count stateflag

ns-consoleloginprompt

The following operations can be performed on "ns-consoleloginprompt":

show| unset| set|

show ns consoleloginprompt

Synopsis

show ns consoleloginprompt

Output

promptString Console login prompt string

Example

get ns consoleloginprompt

unset ns consoleloginprompt

Use this command to remove ns consoleloginprompt settings.Refer to the set ns consoleloginprompt command for meanings of the arguments.

Synopsis

unset ns consoleloginprompt -promptString

set ns consoleloginprompt

Synopsis

set ns consoleloginprompt <promptString>

Arguments

promptString Console login prompt string

Example

set ns consoleloginprompt <prompt_string>

ns-cqaparam

The following operations can be performed on "ns-cqaparam":

show| unset| set|

show ns cqaparam

Displays the values configured for CQA on the appliance.

Synopsis

show ns cqaparam

Arguments

Output

harqretxdelay HARQ retransmission delay (in ms).

net1label Name of the network label.

net2label Name of the network label 2.

minRTTNet1 MIN RTT (in ms) for the first network.

lr1coeflist coefficients values for Label1.

lr1probthresh Probability threshold values for LR model to differentiate between NET1 and reset(NET2 and NET3).

net1cclscale Three congestion level scores limits corresponding to None, Low, Medium.

net1csqscale Three signal quality level scores limits corresponding to Excellent, Good, Fair.

net1logcoef Connection quality ranking Log coefficients of network 1.

minRTTNet2 MIN RTT (in ms) for the second network.

lr2coeflist coefficients values for Label 2.

lr2probthresh Probability threshold values for LR model to differentiate between NET2 and NET3.

net2cclscale Three congestion level scores limits corresponding to None, Low, Medium.

net2csqscale Three signal quality level scores limits corresponding to Excellent, Good, Fair.

net2logcoef Connnection quality ranking Log coefficients of network 2.

net3label Name of the network label 3.

minRTTNet3 MIN RTT (in ms) for the third network.

net3cclscale Three congestion level scores limits corresponding to None, Low, Medium.

net3csqscale Three signal quality level scores limits corresponding to Excellent, Good, Fair.

net3logcoef Connection quality ranking Log coefficients of network 3.

Example

By default, there is no CQA control on the appliance. This control will be hidden and configured using Nitro API using MAS, For the internal testing we are exposing these.

```
show cqa param sh cqaparam Configured CQA parameters: harqretxdelay (in ms): 7
net1label: 2g net1label Coeflist:
intercept=4.95,thruputavg=5.92,iaiavg=-189.48,rttmin=-15.75,loaddelayavg=0.01,noisedelayavg=-2.59
net1label Probthresh: 0.600000 net1label CCL Scale: 25,50,75 net1label CSQ Scale:
25,50,75 net1label CRQ LogCoef: 1.49,3.62,-0.14,1.84,4.83 net1minrtt (in ms): 25 net2label:
3g net2label Coeflist:
intercept=16.4,thruputavg=0.05981,iai1ms=53.27,iai2ms=-50.44,iaiavg=-189.48,isiavg=-203.42,rttmin=-198
net2label Probthresh: 0.500000 net2label CCL Scale: 25,50,75 net2label CSQ Scale:
25,50,75 net2label CRQ LogCoef: 2.39,1.76,-0.08,1.73,4.74 net2minrtt (in ms): 30 net3label:
4g net3label CCL Scale: 25,50,75 net3label CSQ Scale: 25,50,75 net3label CRQ LogCoef:
1.49,3.62,-0.14,1.84,4.83 net3minrtt(in ms): 35
```

```
Done
```

unset ns cqaparam

Use this command to remove ns cqaparam settings.Refer to the set ns cqaparam command for meanings of the arguments.

Synopsis

unset ns cqaparam

set ns cqaparam

Sets the CQA info on the system.

Synopsis

set ns cqaparam

Arguments

harqretxdelay HARQ retransmission delay (in ms). Default value: 0 Minimum value: 1 Maximum value: 64000

net1label Name of the network label.

minRTTNet1 MIN RTT (in ms) for the first network. Default value: 0 Minimum value: 0 Maximum value: 6400

lr1coeflist coefficients values for Label1.

lr1probthresh Probability threshold values for LR model to differentiate between NET1 and reset(NET2 and NET3). Default value: 0 Minimum value: 0 Maximum value: 1

net1cclscale Three congestion level scores limits corresponding to None, Low, Medium.

net1csqscale Three signal quality level scores limits corresponding to Excellent, Good, Fair.

net1logcoef Connection quality ranking Log coefficients of network 1.

net2label Name of the network label 2.

minRTTNet2 MIN RTT (in ms) for the second network. Default value: 0 Minimum value: 0 Maximum value: 6400

lr2coeflist coefficients values for Label 2.

lr2probthresh Probability threshold values for LR model to differentiate between NET2 and NET3. Default value: 0 Minimum value: 0 Maximum value: 1

net2cclscale Three congestion level scores limits corresponding to None, Low, Medium.

net2csqscale Three signal quality level scores limits corresponding to Excellent, Good, Fair.

net2logcoef Connnection quality ranking Log coefficients of network 2.

net3label Name of the network label 3.

minRTTNet3 MIN RTT (in ms) for the third network. Default value: 0 Minimum value: 0 Maximum value: 6400

net3cclscale Three congestion level scores limits corresponding to None, Low, Medium.

net3csqscale Three signal quality level scores limits corresponding to Excellent, Good, Fair.

net3logcoef Connection quality ranking Log coefficients of network 3.

Example

The following command will set CQA info on the system. set ns cqaparam -harqretxdelay 7 -net1label 2g -minRTTNet1 25 -lr1coeflist intercept=4.95,thruputavg=5.92,iaiavg=-189.48,rttmin=-15.75, loaddelayavg=0.01,noisedelayavg=-2.59 -lr1probthresh 6.00e-01 -net1cclscale 25,50,75 -net1csqscale 25,50,75 -net1logcoef 1.49,3.62,-0.14,1.84,4.83 -net2label 3g -minRTTNet2 30 -lr2coeflist intercept=16.4,thruputavg=0.05981,iai1ms=53.27, iai2ms=-50.44,iaiavg=-189.48,isiavg=-203.42,rttmin=-198.42,rttmax=-9.10, rttavg=9.07,loaddelayavg=55.14,noisedelayavg=-68.50 -lr2probthresh 5.00e-01 -net2cclscale 25,50,75 -net2csqscale 25,50,75 -net2logcoef 2.39,1.76,-0.08,1.73,4.74 -net3label 4g -minRTTNet3 35 -net3cclscale 25,50,75 -net3csqscale 25,50,75 -net3logcoef 1.49,3.62,-0.14,1.84,4.83

Feature list: iai1ms, iai2ms, thruputavg, rttavg, bifavg, rcvwndavg loaddelayavg, noisedelayavg, iaiaavg, isiavg, rttmin rttmax

The 'show ns cqa param' command can be used to view the current settings of the CQA.

```
show ns cqaparam Done
```

ns-dhcpIp

The following operations can be performed on "ns-dhcpIp":

release ns dhcpIp

Releases the IP address acquired by the DHCP client.

Synopsis

release ns dhcpIp

ns-dhcpParams

The following operations can be performed on "ns-dhcpParams":

show| unset| set|

show ns dhcpParams

Displays the parameters configured for the DHCP client.

Synopsis

show ns dhcpParams

Arguments

Output

dhcpClient ON, if DHCP client active on next reboot, else OFF

IPAddress DHCP acquired IP

netmask DHCP acquired Netmask

hostRtGw DHCP acquired Gateway

running DHCP mode

saveroute DHCP acquired gateway save flag

unset ns dhcpParams

Use this command to remove ns dhcpParams settings.Refer to the set ns dhcpParams command for meanings of the arguments.

Synopsis

unset ns dhcpParams

set ns dhcpParams

Sets the DHCP client parameters.

Synopsis

set ns dhcpParams

Arguments

dhcpClient Enables DHCP client to acquire IP address from the DHCP server in the next boot. When set to OFF, disables the DHCP client in the next boot.

Possible values: ON, OFF Default value: OFF

saveroute DHCP acquired routes are saved on the Citrix ADC.

Possible values: ON, OFF Default value: OFF

ns-diameter

The following operations can be performed on "ns-diameter":

unset| set| show|

unset ns diameter

Use this command to remove ns diameter settings.Refer to the set ns diameter command for meanings of the arguments.

Synopsis

unset ns diameter

set ns diameter

Set the diameter configuration on NS.

Synopsis

set ns diameter

Arguments

identity DiameterIdentity to be used by NS. DiameterIdentity is used to identify a Diameter node uniquely. Before setting up diameter configuration, Citrix ADC (as a Diameter node) MUST be assigned a unique DiameterIdentity. example => set ns diameter -identity netscaler.com Now whenever Citrix ADC needs to use identity in diameter messages. It will use 'netscaler.com' as Origin-Host AVP as defined in RFC3588

realm Diameter Realm to be used by NS. example => set ns diameter -realm com Now whenever Citrix ADC system needs to use realm in diameter messages. It will use 'com' as Origin-Realm AVP as defined in RFC3588

serverClosePropagation when a Server connection goes down, whether to close the corresponding client connection if there were requests pending on the server.

Possible values: YES, NO Default value: NO

ownerNode ID of the cluster node for which the diameter id is set, can be configured only through CLIP Default value: -1 Minimum value: 0 Maximum value: 31

show ns diameter

Displays the diameter parameters configured on the Citrix ADC.

Synopsis

show ns diameter

Arguments

ownerNode ID of the cluster node for which the diameter id is set, can be configured only through CLIP Default value: -1 Minimum value: 0 Maximum value: 31

Output

identity DiameterIdentity to be used by NS. DiameterIdentity is used to identify a Diameter node uniquely. Before setting up diameter configuration, Citrix ADC (as a Diameter node) MUST be assigned a unique DiameterIdentity. example => set ns diameter -identity netscaler.com Now whenever Citrix ADC needs to use identity in diameter messages. It will use 'netscaler.com' as Origin-Host AVP as defined in RFC3588

realm Diameter Realm to be used by NS. example => set ns diameter -realm com Now whenever Citrix ADC system needs to use realm in diameter messages. It will use 'com' as Origin-Realm AVP as defined in RFC3588

serverClosePropagation when a Server connection goes down, whether to close the corresponding client connection if there were requests pending on the server.

devno count stateflag

ns-encryptionKey

The following operations can be performed on "ns-encryptionKey":

set| show| rm| add| unset|

set ns encryptionKey

Change parameters for an existing encryption key, If the method is changed, the keyVAlue must also be changed.

Synopsis

set ns encryptionKey <name>

Arguments

name Key name. This follows the same syntax rules as other expression entity names: It must begin with an alpha character (A-Z or a-z) or an underscore (_). The rest of the characters must be alpha, numeric (0-9) or underscores. It cannot be re or xp (reserved for regular and XPath expressions). It cannot be an expression reserved word (e.g. SYS or HTTP). It cannot be used for an existing expression object (HTTP callout, patset, dataset, stringmap, or named expression).

method Cipher method to be used to encrypt and decrypt content. NONE - no encryption or decryption is performed The output of ENCRYPT() and DECRYPT() is the same as the input. RC4 - the RC4 stream cipher with a 128 bit (16 byte) key; RC4 is now considered insecure and should only be used if required by existing applciations. DES - the Data Encryption Standard (DES) block cipher with a 64-bit (8 byte) key, with 56 data bits and 8 parity bits. DES is considered less secure than DES3 or AES so it should only be used if required by an existing applicastion. The optional mode is described below; DES without a mode is equivalent to DES-CBC. DES3 - the Triple Data Encryption Standard (DES) block cipher with a 192-bit (24 byte) key. The optional mode is described below; DES3 without a mode is equivalent to DES3-CBC. AES<keysize> - the Advanced Encryption Standard block cipher, available with 128 bit (16 byte), 192 bit (24 byte), and 256 bit (32 byte) keys. The optional mode is described below; AES<keysize> without a mode is equivalent to AES<keysize>-CBC.

For a block cipher, the <mode> specifies how multiple blocks of plaintext are encrypted and how the Initialization Vector (IV) is used. Choices are CBC (Cipher Block Chaining) - Each block of plaintext is XORed with the previous ciphertext block, or IV for the first block, before being encrypted. Padding is required if the plaintext is not a multiple of the cipher block size. CFB (Cipher Feedback) - The previous ciphertext block, or the IV for the first block, is encrypted and the output is XORed with the current plaintext block to create the current ciphertext block. The 128-bit version of CFB is provided. Padding is not required. OFB (Output Feedback) - A keystream is generated by applying the cipher successfully to the IV and XORing the keystream blocks with the plaintext. Padding is not required. ECB (Electronic Codebook) - Each block of plaintext is independently encrypted. An IV is not used. Padding is required. This mode is considered less secure than the other modes because the same plaintext always produces the same encrypted text and should only be used if required by an existing application.

Possible values: NONE, RC4, DES3, AES128, AES192, AES256, DES, DES-CBC, DES-CFB, DES-OFB, DES-ECB, DES3-CBC, DES3-CFB, DES3-OFB, DES3-ECB, AES128-CBC, AES128-CFB, AES128-OFB, AES128-ECB, AES192-CBC, AES192-CFB, AES192-OFB, AES192-ECB, AES256-CBC, AES256-CFB, AES256-OFB, AES256-ECB

keyValue The hex-encoded key value. The length is determined by the cipher method: RC4 - 16 bytes DES - 8 bytes (all modes) DES3 - 24 bytes (all modes) AES128 - 16 bytes (all modes) AES192 - 24 bytes (all modes) AES256 - 32 bytes (all modes) Note that the keyValue will be encrypted when it it is saved.

There is a special key value AUTO which generates a new random key for the specified method. This kind of key is intended for use cases where the NetScaler both encrypts and decrypts the same data, such an HTTP header.

padding Enables or disables the padding of plaintext to meet the block size requirements of block ciphers: ON - For encryption, PKCS5/7 padding is used, which appends n bytes of value n on the end of the plaintext to bring it to the cipher block lnegth. If the plaintext length is alraady a multiple of the block length, an additional block with bytes of value block_length will be added. For decryption, ISO 10126 padding is accepted, which expects the last byte of the block to be the number of added pad bytes. Note that this accepts PKCS5/7 padding, as well as ANSI_X923 padding. Padding ON is the default for the ECB and CBD modes. OFF - No padding. An Undef error will occur with the ECB or CBC modes if the plaintext length is not a multitple of the cipher block size. This can be used with the CFB and OFB modes, and with the ECB and CBC modes if the plaintext will always be an integral number of blocks, or if custom padding is implemented using a policy extension function. Padding OFf is the default for CFB and OFB modes.

Possible values: OFF, ON Default value: DEFAULT

iv The initalization voector (IV) for a block cipher, one block of data used to initialize the encryption. The best practice is to not specify an IV, in which case a new random IV will be generated for each encryption. The format must be iv_data or keyid_iv_data to include the generated IV in the encrypted data. The IV should only be specified if it cannot be included in the encrypted data. The IV length is the cipher block size: RC4 - not used (error if IV is specified) DES - 8 bytes (all modes) DES3 - 8 bytes (all modes) AES128 - 16 bytes (all modes) AES192 - 16 bytes (all modes) AES256 - 16 bytes (all modes)

comment Comments associated with this encryption key.

Example

set ns encryptionKey my_key -keyValue b8742b163abcf62d639837bbee3cef9fb5842d82d00dfe6548831d2bd1d93476

show ns encryptionKey

Display configured encryption keys

Synopsis

show ns encryptionKey

Arguments

name Key name. This follows the same syntax rules as other expression entity names: It must begin with an alpha character (A-Z or a-z) or an underscore (_). The rest of the characters must be alpha, numeric (0-9) or underscores. It cannot be re or xp (reserved for regular and XPath expressions). It cannot be an expression reserved word (e.g. SYS or HTTP). It cannot be used for an existing expression object (HTTP callout, patset, dataset, stringmap, or named expression).

Output

method Cipher method to be used to encrypt and decrypt content. NONE - no encryption or decryption is performed The output of ENCRYPT() and DECRYPT() is the same as the input. RC4 - the RC4 stream cipher with a 128 bit (16 byte) key; RC4 is now considered insecure and should only be used if required by existing applciations. DES - the Data Encryption Standard (DES) block cipher with a 64-bit (8 byte) key, with 56 data bits and 8 parity bits. DES is considered less secure than DES3 or AES so it should only be used if required by an existing applicastion. The optional mode is described below; DES without a mode is equivalent to DES-CBC. DES3 - the Triple Data Encryption Standard (DES) block cipher with a 192-bit (24 byte) key. The optional mode is

described below; DES3 without a mode is equivalent to DES3-CBC. AES<keysize> - the Advanced Encryption Standard block cipher, available with 128 bit (16 byte), 192 bit (24 byte), and 256 bit (32 byte) keys. The optional mode is described below; AES<keysize> without a mode is equivalent to AES<keysize>-CBC.

For a block cipher, the <mode> specifies how multiple blocks of plaintext are encrypted and how the Initialization Vector (IV) is used. Choices are CBC (Cipher Block Chaining) - Each block of plaintext is XORed with the previous ciphertext block, or IV for the first block, before being encrypted. Padding is required if the plaintext is not a multiple of the cipher block size. CFB (Cipher Feedback) - The previous ciphertext block, or the IV for the first block, is encrypted and the output is XORed with the current plaintext block to create the current ciphertext block. The 128-bit version of CFB is provided. Padding is not required. OFB (Output Feedback) - A keystream is generated by applying the cipher successfully to the IV and XORing the keystream blocks with the plaintext. Padding is not required. ECB (Electronic Codebook) - Each block of plaintext is independently encrypted. An IV is not used. Padding is required. This mode is considered less secure than the other modes because the same plaintext always produces the same encrypted text and should only be used if required by an existing application.

keyValue The hex-encoded key value. The length is determined by the cipher method: RC4 - 16 bytes DES - 8 bytes (all modes) DES3 - 24 bytes (all modes) AES128 - 16 bytes (all modes) AES192 - 24 bytes (all modes) AES256 - 32 bytes (all modes) Note that the keyValue will be encrypted when it it is saved.

There is a special key value AUTO which generates a new random key for the specified method. This kind of key is intended for use cases where the NetScaler both encrypts and decrypts the same data, such an HTTP header.

padding Enables or disables the padding of plaintext to meet the block size requirements of block ciphers: ON - For encryption, PKCS5/7 padding is used, which appends n bytes of value n on the end of the plaintext to bring it to the cipher block lnegth. If the plaintext length is alraady a multiple of the block length, an additional block with bytes of value block_length will be added. For decryption, ISO 10126 padding is accepted, which expects the last byte of the block to be the number of added pad bytes. Note that this accepts PKCS5/7 padding, as well as ANSI_X923 padding. Padding ON is the default for the ECB and CBD modes. OFF - No padding. An Undef error will occur with the ECB or CBC modes if the plaintext length is not a multitple of the cipher block size. This can be used with the CFB and OFB modes, and with the ECB and CBC modes if the plaintext will always be an integral number of blocks, or if custom padding is implemented using a policy extension function. Padding OFf is the default for CFB and OFB modes.

iv The initalization voector (IV) for a block cipher, one block of data used to initialize the encryption. The best practice is to not specify an IV, in which case a new random IV will be generated for each encryption. The format must be iv_data or keyid_iv_data to include the generated IV in the encrypted data. The IV should only be specified if it cannot be included in the encrypted data. The IV length is the cipher block size: RC4 - not used (error if IV is specified) DES - 8 bytes (all modes) DES3 - 8 bytes (all modes) AES128 - 16 bytes (all modes) AES192 - 16 bytes (all modes) AES256 - 16 bytes (all modes)

comment Comments associated with this encryption key.

stateflag devno count

rm ns encryptionKey

Remove an encryption key. There can be no existing ENCRYPT() or DECRYPT() functions that use the key.

Synopsis

rm ns encryptionKey <name>

Arguments

name Key name. This follows the same syntax rules as other expression entity names: It must begin with an alpha character (A-Z or a-z) or an underscore (_). The rest of the characters must be alpha, numeric (0-9) or underscores. It cannot be re or xp (reserved for regular and XPath expressions). It cannot be an expression reserved word (e.g. SYS or HTTP). It cannot be used for an existing expression object (HTTP callout, patset, dataset, stringmap, or named expression).

Example

rm ns encryptionKey my_key

add ns encryptionKey

Create a key to be used in ENCRYPT() and DECRYPT() policy functions.

Synopsis

add ns encryptionKey <name> -method <method>

Arguments

name Key name. This follows the same syntax rules as other expression entity names: It must begin with an alpha character (A-Z or a-z) or an underscore (_). The rest of the characters must be alpha, numeric (0-9) or underscores. It cannot be re or xp (reserved for regular and XPath expressions). It cannot be an expression reserved word (e.g. SYS or HTTP). It cannot be used for an existing expression object (HTTP callout, patset, dataset, stringmap, or named expression).

method Cipher method to be used to encrypt and decrypt content. NONE - no encryption or decryption is performed The output of ENCRYPT() and DECRYPT() is the same as the input. RC4 - the RC4 stream cipher with a 128 bit (16 byte) key; RC4 is now considered insecure and should only be used if required by existing applciations. DES - the Data Encryption Standard (DES) block cipher with a 64-bit (8 byte) key, with 56 data bits and 8 parity bits. DES is considered less secure than DES3 or AES so it should only be used if required by an existing applicastion. The optional mode is described below; DES without a mode is equivalent to DES-CBC. DES3 - the Triple Data Encryption Standard (DES) block cipher with a 192-bit (24 byte) key. The optional mode is described below; DES3 without a mode is equivalent to DES3-CBC. AES<keysize> - the Advanced Encryption Standard block cipher, available with 128 bit (16 byte), 192 bit (24 byte), and 256 bit (32 byte) keys. The optional mode is described below; AES<keysize> without a mode is equivalent to AES<keysize>-CBC.

For a block cipher, the <mode> specifies how multiple blocks of plaintext are encrypted and how the Initialization Vector (IV) is used. Choices are CBC (Cipher Block Chaining) - Each block of plaintext is XORed with the previous ciphertext block, or IV for the first block, before being encrypted. Padding is required if the plaintext is not a multiple of the cipher block size. CFB (Cipher Feedback) - The previous ciphertext block, or the IV for the first block, is encrypted and the output is XORed with the current plaintext block to create the current ciphertext block. The 128-bit version of CFB is provided. Padding is not required. OFB (Output Feedback) - A keystream is generated by applying the cipher successfully to the IV and XORing the keystream blocks with the plaintext. Padding is not required. ECB (Electronic Codebook) - Each block of plaintext is independently encrypted. An IV is not used. Padding is required. This mode is considered less secure than the other modes because the same plaintext always produces the same encrypted text and should only be used if required by an existing application.

Possible values: NONE, RC4, DES3, AES128, AES192, AES256, DES, DES-CBC, DES-CFB, DES-OFB, DES-ECB, DES3-CBC, DES3-CFB, DES3-OFB, DES3-ECB, AES128-CBC, AES128-CFB, AES128-OFB, AES128-ECB, AES192-CBC, AES192-CFB, AES192-OFB, AES192-ECB, AES256-CBC, AES256-CFB, AES256-OFB, AES256-ECB

keyValue The hex-encoded key value. The length is determined by the cipher method: RC4 - 16 bytes DES - 8 bytes (all modes) DES3 - 24 bytes (all modes) AES128 - 16 bytes (all modes) AES192 - 24 bytes (all modes) AES256 - 32 bytes (all modes) Note that the keyValue will be encrypted when it it is saved.

There is a special key value AUTO which generates a new random key for the specified method. This kind of key is intended for use cases where the NetScaler both encrypts and decrypts the same data, such an HTTP header.

padding Enables or disables the padding of plaintext to meet the block size requirements of block ciphers: ON - For encryption, PKCS5/7 padding is used, which appends n bytes of value n on the end of the plaintext to bring it to the cipher block lnegth. If the plaintext length is alraady a multiple of the block length, an additional block with bytes of value block_length will be added. For decryption, ISO 10126 padding is accepted, which expects the last byte of the block to be the number of added pad bytes. Note that this accepts PKCS5/7 padding, as well as ANSI_X923 padding. Padding ON is the default for the ECB and CBD modes. OFF - No padding. An Undef error will occur with the ECB or CBC modes if the plaintext length is not a multitple of the cipher block size. This can be used with the CFB and OFB modes, and with the ECB and CBC modes if the plaintext will always be an integral number of blocks, or if custom padding is implemented using a policy extension function. Padding OFf is the default for CFB and OFB modes.

Possible values: OFF, ON Default value: DEFAULT

iv The initalization voector (IV) for a block cipher, one block of data used to initialize the encryption. The best practice is to not specify an IV, in which case a new random IV will be generated for each encryption. The format must be iv_data or keyid_iv_data to include the generated IV in the encrypted data. The IV should only be specified if it cannot be included in the encrypted data. The IV length is the cipher block size: RC4 - not used (error if IV is specified) DES - 8 bytes (all modes) DES3 - 8 bytes (all modes) AES128 - 16 bytes (all modes) AES192 - 16 bytes (all modes) AES256 - 16 bytes (all modes)

comment Comments associated with this encryption key.

Example

add ns encryptionKey my_key -method aes256 -keyValue 26ea5537b7e0746089476e5658f9327c0b10c3b4778c673a5b38cee182874711

unset ns encryptionKey

Use this command to remove ns encryptionKey settings.Refer to the set ns encryptionKey command for meanings of the arguments.

Synopsis

unset ns encryptionKey <name>

ns-encryptionParams

The following operations can be performed on "ns-encryptionParams":

show| set|

show ns encryptionParams

Displays the encryption method configured on the Citrix ADC.

Synopsis

show ns encryptionParams

Arguments

Output

method The cipher method (and key length) used to encrypt and decrypt content.

keyValue The base64-encoded key generation number, method, and key value. Note:

- Do not include this argument if you are changing the encryption method.
- To generate a new key value for the current encryption method, specify an empty string \(""\) as the value of this parameter. The parameter is passed implicitly, with its automatically generated value, to the Citrix ADC packet engines even when it is not included in the command. Passing the parameter to the packet engines enables the appliance to save the key value to the configuration file and to propagate the key value to the secondary appliance in a high availability setup.

set ns encryptionParams

Sets the parameters required for encrypting or decrypting content.

Synopsis

set ns encryptionParams -method <method>

Arguments

method Cipher method (and key length) to be used to encrypt and decrypt content. The default value is AES256.

Possible values: NONE, RC4, DES3, AES128, AES192, AES256, DES, DES-CBC, DES-CFB, DES-OFB, DES-ECB, DES3-CBC, DES3-CFB, DES3-OFB, DES3-ECB, AES128-CBC, AES128-CFB, AES128-OFB, AES128-ECB, AES192-CBC, AES192-CFB, AES192-OFB, AES192-ECB, AES256-CBC, AES256-CFB, AES256-OFB, AES256-ECB

keyValue The base64-encoded key generation number, method, and key value. Note:

- Do not include this argument if you are changing the encryption method.
- To generate a new key value for the current encryption method, specify an empty string \(""\) as the value of this parameter. The parameter is passed implicitly, with its automatically generated value, to the Citrix ADC packet engines even when it is not included in the command. Passing the parameter to the packet engines enables the appliance to save the key value to the configuration file and to propagate the key value to the secondary appliance in a high availability setup.

Example

set ns encryptionParams -method aes128

ns-events

The following operations can be performed on "ns-events":

show ns events

Displays events that occur on the appliance.

Synopsis

show ns events

Arguments

eventNo Event number starting from which events must be shown. Minimum value: 0

Output

time Event no.

eventcode event Code.

devid Device Name.

devname Device Name.

text Event no.

data0 additional event information.

data1 additional event information.

data2 additional event information.

data3 additional event information.

devno count stateflag

Example

show ns events

ns-extension

The following operations can be performed on "ns-extension":

import| show| update| add| rm| unset| set|

import ns extension

Imports the specified extension to the Citrix ADC, assigns it the specified name, and stores it in the list of extension objects.

Synopsis

import ns extension <src> <name>

Arguments

src Local path to and name of, or URL (protocol, host, path, and file name) for, the file in which to store the imported extension. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

name Name to assign to the extension object on the Citrix ADC.

comment Any comments to preserve information about the extension object.

overwrite Overwrites the existing file

Example

import ns extension http://www.example.com/extension.lua my-extension

show ns extension

Displays the specified extension object.

Synopsis

show ns extension

Arguments

name Name of the extension object.

detail Show detail for extension function.

Possible values: brief, all

Output

stateflag src Local path to and name of, or URL (protocol, host, path, and file name) for, the file in which to store the imported extension. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

type extensionFunctionName Name of extension function given in the extension.

extensionFunctionLineNumber Line number of the function in file.

extensionFunctionClassType Extension function class type.

extensionFunctionClasses List of classes (including inherited) that the function is present in.

extensionFunctionClassesCount Number of classes the function is present in.

extensionFunctionReturnType Extension function return type.

activeExtensionFunction Extension function is in use or not.

extensionFunctionArgType List of extension function's arguments types

extensionFunctionAllParams List of parameters (including promotions) that the function can accept.

extensionFunctionAllParamsCount Number of parameters (including promotions) that the function can accept.

extensionFuncDescription Any description to preserve information about the extension function.

extensionFunctionArgCount Number of parameters in the extension function

comment Any comments to preserve information about the extension object.

functionHits Number of time function evaluates successfully.

functionUndefHits Number of times error occured in evaluating extension function.

functionHaltCount Number of time function evaluation is halted.

trace Enables tracing to the NS log file of extension execution: off - turns off tracing (equivalent to unset ns extension <extension-name> -trace) calls - traces extension function calls with arguments and function returns with the first return value lines - traces the above plus line numbers for executed extension lines all - traces the above plus local variables changed by executed extension lines Note that the DEBUG log level must be enabled to see extension tracing. This can be done by set audit syslogParams -loglevel ALL or -loglevel DEBUG.

traceFunctions Comma-separated list of extension functions to trace. By default, all extension functions are traced.

traceVariables Comma-separated list of variables (in traced extension functions) to trace. By default, all variables are traced.

devno count

Example

show ns extension my-extension

update ns extension

Update the specified extension object.

Synopsis

update ns extension <name>

Arguments

name Name to assign to the extension object on the Citrix ADC.

Example

update ns extension my-extension

add ns extension

Add the specified extension object.

Synopsis

add ns extension <name>

Arguments

name Name to assign to the extension object on the Citrix ADC.

comment Any comments to preserve information about the extension object.

Example

add ns extension my-extension

rm ns extension

Removes the specified extension object.

Synopsis

rm ns extension <name>

Arguments

name Name of the extension object to remove.

Example

rm ns extension my-extension

unset ns extension

Use this command to remove ns extension settings.Refer to the set ns extension command for meanings of the arguments.

Synopsis

unset ns extension <name>

set ns extension

Modifies properties of the extension, including the comment and tracing. Note that tracing parameters are not preserved by a save config and so do not survive a reboot.

Synopsis

set ns extension <name>

Arguments

name Name to assign to the extension object on the Citrix ADC.

trace Enables tracing to the NS log file of extension execution: off - turns off tracing (equivalent to unset ns extension <extension-name> -trace) calls - traces extension function calls with arguments and function returns with the first return value lines - traces the above plus line numbers for executed extension lines all - traces the above plus local variables changed by executed extension lines Note that the DEBUG log level must be enabled to see extension tracing. This can be done by set audit syslogParams -loglevel ALL or -loglevel DEBUG.

Possible values: off, calls, lines, all Default value: off

traceFunctions Comma-separated list of extension functions to trace. By default, all extension functions are traced.

traceVariables Comma-separated list of variables (in traced extension functions) to trace. By default, all variables are traced.

comment Any comments to preserve information about the extension object.

Example

set ns extension <extension name> -tracing all

ns-feature

The following operations can be performed on "ns-feature":

enable| disable| show|

enable ns feature

Enables Citrix ADC feature(s).

Synopsis

enable ns feature <feature> ...

Arguments

feature Feature to be enabled. Multiple features can be specified by providing a blank space between each feature.

Example

enable ns feature cs This CLI command enables the Content Switching feature.

disable ns feature

Disables Citrix ADC feature(s).

Synopsis

disable ns feature <feature> ...

Arguments

feature Feature to be disabled. Multiple features can be specified by providing a blank space between each feature.

Related Commands

- disable ns mode

show ns feature

Displays the current state of Citrix ADC features.

Synopsis

show ns feature

Arguments

Output

feature Feature to be enabled. Multiple features can be specified by providing a blank space between each feature.

WL Web Logging.

SP Surge Protection.

LB Load Balancing.

CS Content Switching.

CR Cache Redirect.

CMP Compression.

SSL Secure Sockets Layer.

GSLB Global Server Load Balancing.

Routing Routing.

CF Content Filter.

IC Integrated Caching.

SSLVPN SSL VPN.

AAA AAA

OSPF OSPF Routing.

RIP RIP Routing.

BGP BGP Routing.

REWRITE Rewrite.

IPv6PT IPv6 protocol translation

AppFw Application Firewall.

RESPONDER Responder.

push Citrix ADC Push.

AppFlow AppFlow.

CloudBridge CloudBridge.

ISIS ISIS Routing.

CH Call Home.

AppQoE AppQoS

DiskCaching Integrated Disk Cache

ContentAccelerator Transparent Integrated Caching.

FEO Optimize Web content (HTML, CSS, JavaScript, images)

LSN Large Scale NAT.

RDPProxy RDPPROXY.

Rep Reputation Services.

URLFiltering URL Filtering.

VideoOptimization Video Optimization.

ForwardProxy Forward Proxy.

SSLInterception SSL Interception.

AdaptiveTCP Adaptive TCP.

CQA Connection Quality Analytics.

CI Content Inspection.

Bot Bot Management.

APIGateway API Gateway

ns-hardware

The following operations can be performed on "ns-hardware":

show ns hardware

Displays details of the appliance hardware and information such as the host ID and the serial number.

Synopsis

show ns hardware

Arguments

Output

hwdescription Hardware and it's ports detail.

sysId System id.

manufactureDay Manufacturing day.

manufactureMonth Manufacturing month.

manufactureYear Manufacturing year.

cpufrequncy CPU Frequency.

hostId host id.

host host id.

serialNo Serial no.

encodedSerialNo Encoded serial no.

netscalerUUID Citrix ADC UUID

bmcRevision BMC Firmware Revision

ns-hmacKey

The following operations can be performed on "ns-hmacKey":

add| rm| unset| show| set|

add ns hmacKey

Create a key to be used in HMAC() policy functions.

Synopsis

add ns hmacKey <name> -digest <digest>

Arguments

name Key name. This follows the same syntax rules as other expression entity names: It must begin with an alpha character (A-Z or a-z) or an underscore (_). The rest of the characters must be alpha, numeric (0-9) or underscores. It cannot be re or xp (reserved for regular and XPath expressions). It cannot be an expression reserved word (e.g. SYS or HTTP). It cannot be used for an existing expression object (HTTP callout, patset, dataset, stringmap, or named expression).

digest Digest (hash) function to be used in the HMAC computation.

Possible values: MD2, MD4, MD5, SHA1, SHA224, SHA256, SHA384, SHA512

keyValue The hex-encoded key to be used in the HMAC computation. The key can be any length (up to a Citrix ADC-imposed maximum of 255 bytes). If the length is less than the digest block size, it will be zero padded up to the block size. If it is greater than the block size, it will be hashed using the digest function to the block size. The block size for each digest is: MD2 - 16 bytes MD4 - 16 bytes MD5 - 16 bytes SHA1 - 20 bytes SHA224 - 28 bytes SHA256 - 32 bytes SHA384 - 48 bytes SHA512 - 64 bytes Note that the key will be encrypted when it it is saved

There is a special key value AUTO which generates a new random key for the specified digest. This kind of key is intended for use cases where the NetScaler both generates and verifies an HMAC on the same data.

comment Comments associated with this encryption key.

Example

add ns hmacKey my_hmac_key -digest sha1 -keyValue 0c753c6c5ef859189cacdf95b506d02c1797407d

rm ns hmacKey

Remove an HMACkey. There can be no existing HMAC() functions that use the key.

Synopsis

rm ns hmacKey <name>

Arguments

name Key name. This follows the same syntax rules as other expression entity names: It must begin with an alpha character (A-Z or a-z) or an underscore (_). The rest of the characters must be alpha, numeric (0-9) or underscores. It cannot be re or xp (reserved for regular and XPath expressions). It cannot be an expression reserved word (e.g. SYS or HTTP). It cannot be used for an existing expression object (HTTP callout, patset, dataset, stringmap, or named expression).

Example

rm ns hmacKey my_hmac_key

unset ns hmacKey

Use this command to remove ns hmacKey settings.Refer to the set ns hmacKey command for meanings of the arguments.

Synopsis

unset ns hmacKey <name> -comment

show ns hmacKey

Display configured HMAC keys

Synopsis

show ns hmacKey

Arguments

name Key name. This follows the same syntax rules as other expression entity names: It must begin with an alpha character (A-Z or a-z) or an underscore (_). The rest of the characters must be alpha, numeric (0-9) or underscores. It cannot be re or xp (reserved for regular and XPath expressions). It cannot be an expression reserved word (e.g. SYS or HTTP). It cannot be used for an existing expression object (HTTP callout, patset, dataset, stringmap, or named expression).

Output

digest Digest (hash) function to be used in the HMAC computation.

keyValue The hex-encoded key to be used in the HMAC computation. The key can be any length (up to a Citrix ADC-imposed maximum of 255 bytes). If the length is less than the digest block size, it will be zero padded up to the block size. If it is greater than the block size, it will be hashed using the digest function to the block size. The block size for each digest is: MD2 - 16 bytes MD4 - 16

bytes MD5 - 16 bytes SHA1 - 20 bytes SHA224 - 28 bytes SHA256 - 32 bytes SHA384 - 48 bytes SHA512 - 64 bytes Note that the key will be encrypted when it it is saved

There is a special key value AUTO which generates a new random key for the specified digest. This kind of key is intended for use cases where the NetScaler both generates and verifies an HMAC on the same data.

comment Comments associated with this encryption key.

stateflag devno count

set ns hmacKey

Change an existing HMAC key.

Synopsis

set ns hmacKey <name>

Arguments

name Key name. This follows the same syntax rules as other expression entity names: It must begin with an alpha character (A-Z or a-z) or an underscore (_). The rest of the characters must be alpha, numeric (0-9) or underscores. It cannot be re or xp (reserved for regular and XPath expressions). It cannot be an expression reserved word (e.g. SYS or HTTP). It cannot be used for an existing expression object (HTTP callout, patset, dataset, stringmap, or named expression).

digest Digest (hash) function to be used in the HMAC computation.

Possible values: MD2, MD4, MD5, SHA1, SHA224, SHA256, SHA384, SHA512

keyValue The hex-encoded key to be used in the HMAC computation. The key can be any length (up to a Citrix ADC-imposed maximum of 255 bytes). If the length is less than the digest block size, it will be zero padded up to the block size. If it is greater than the block size, it will be hashed using the digest function to the block size. The block size for each digest is: MD2 - 16 bytes MD4 - 16 bytes MD5 - 16 bytes SHA1 - 20 bytes SHA224 - 28 bytes SHA256 - 32 bytes SHA384 - 48 bytes SHA512 - 64 bytes Note that the key will be encrypted when it it is saved

There is a special key value AUTO which generates a new random key for the specified digest. This kind of key is intended for use cases where the NetScaler both generates and verifies an HMAC on the same data.

comment Comments associated with this encryption key.

Example

set ns hmacKey my_hmac_key -keyValue f348c594341a840a1f641a1cf24aa24c15eb1317

ns-hostName

The following operations can be performed on "ns-hostName":

set| show|

set ns hostName

Sets the hostname for the Citrix ADC. The hostname is displayed on the shell prompt.

Synopsis

set ns hostName <hostName>

Arguments

hostName Host name for the Citrix ADC.

ownerNode ID of the cluster node for which you are setting the hostname. Can be configured only through the cluster IP address. Default value: 255 Minimum value: 0 Maximum value: 31

Example

set ns hostname nspri

show ns hostName

Displays the host name of the system.

Synopsis

show ns hostName

Arguments

Output

hostName Host name

ownerNode ID of the cluster node for which you are setting the hostname. Can be configured only through the cluster IP address.

devno count stateflag

Example

show ns hostname

ns-httpParam

The following operations can be performed on "ns-httpParam":

show| set| unset|

show ns httpParam

Displays the HTTP parameters configured on the Citrix ADC.

Synopsis

show ns httpParam

Arguments

Output

dropInvalReqs Drop invalid HTTP requests or responses.

markHttp09Inval Mark HTTP/0.9 requests as invalid.

markConnReqInval Mark CONNECT requests as invalid.

insNsSrvrHdr Enable or disable Citrix ADC server header insertion for Citrix ADC generated HTTP responses.

nsSrvrHdr The server header value to be inserted. If no explicit header is specified then NSBUILD.RELEASE is used as default server header.

logErrResp Whether to log HTTP error responses

conMultiplex Reuse server connections for requests from more than one client connections.

maxReusePool Maximum limit on the number of connections, from the Citrix ADC to a particular server that are kept in the reuse pool. This setting is helpful for optimal memory utilization and for reducing the idle connections to the server just after the peak time.

http2ServerSide Enable/Disable HTTP/2 on server side

builtin Flag to determine if the http param is built-in or not

feature The feature to be checked while applying this config

ignoreConnectCodingScheme Ignore Coding scheme in CONNECT request.

set ns httpParam

Sets the configurable HTTP parameters for the Citrix ADC.

Synopsis

set ns httpParam [-insNsSrvrHdr (ON | OFF)]

Arguments

dropInvalReqs Drop invalid HTTP requests or responses.

Possible values: ON, OFF Default value: OFF

markHttp09Inval Mark HTTP/0.9 requests as invalid.

Possible values: ON, OFF Default value: OFF

markConnReqInval Mark CONNECT requests as invalid.

Possible values: ON, OFF Default value: OFF

insNsSrvrHdr Enable or disable Citrix ADC server header insertion for Citrix ADC generated HTTP responses.

Possible values: ON, OFF Default value: OFF

nsSrvrHdr The server header value to be inserted. If no explicit header is specified then NSBUILD.RELEASE is used as default server header.

logErrResp Server header value to be inserted.

Possible values: ON, OFF Default value: ON

conMultiplex Reuse server connections for requests from more than one client connections.

Possible values: ENABLED, DISABLED Default value: ENABLED

maxReusePool Maximum limit on the number of connections, from the Citrix ADC to a particular server that are kept in the reuse pool. This setting is helpful for optimal memory utilization and for

reducing the idle connections to the server just after the peak time. Default value: 0 Minimum value: 0 Maximum value: 360000

http2ServerSide Enable/Disable HTTP/2 on server side

Possible values: ON, OFF Default value: OFF

ignoreConnectCodingScheme Ignore Coding scheme in CONNECT request.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set ns httpParam -dropInvalReqs ON

unset ns httpParam

Use this command to remove ns httpParam settings.Refer to the set ns httpParam command for meanings of the arguments.

Synopsis

unset ns httpParam

ns-httpProfile

The following operations can be performed on "ns-httpProfile":

show| add| set| rm| unset|

show ns httpProfile

Displays information about HTTP profiles configured on the appliance.

Synopsis

show ns httpProfile

Arguments

name Name of the HTTP profile to be displayed. If a name is not provided, information about all HTTP profiles is shown.

Output

dropInvalReqs Dropping of invalid HTTP requests/responses

markHttp09Inval Invalidating HTTP 0.9 requests

markConnReqInval Invalidating CONNECT HTTP requests

markTraceReqInval Invalidating TRACE HTTP requests

markRfc7230NonCompliantInval Invalidating RFC7230 Non-Compliant

markHTTPHeaderExtraWSError Mark Http header with extra white space as invalid

cmpOnPush Compression on PUSH packet

conMultiplex Reuse server connections for requests from more than one client connections.

maxReusePool Maximum connections in reusepool

webSocket HTTP connection to be upgraded to a web socket connection. Once upgraded, Citrix ADC does not process Layer 7 traffic on this connection.

refCnt Number of entities using this profile

stateflag State flag

dropExtraCRLF Drop any extra 'CR' and 'LF' characters present after the header.

incompHdrDelay Maximum time to wait, in milliseconds, between incomplete header packets. If the header packets take longer to arrive at Citrix ADC, the connection is silently dropped.

reqTimeout Time, in seconds, within which the HTTP request must complete. If the request does not complete within this time, the specified request timeout action is executed. Zero disables the timeout.

adptTimeout Adapts the configured request timeout based on flow conditions. The timeout is increased or decreased internally and applied on the flow.

reqTimeoutAction Action to take when the HTTP request does not complete within the specified request timeout duration. You can configure the following actions:

- RESET - Send RST (reset) to client when timeout occurs.
- DROP - Drop silently when timeout occurs.
- Custom responder action - Name of the responder action to trigger when timeout occurs, used to send custom message.

dropExtraData Drop any extra data when server sends more data than the specified content-length.

webLog Disabling weblog option

clientIpHdrExpr Name of the header that contains the real client IP address.

maxReq Maximum number of requests allowed on a single connection. Zero implies no limit on the number of requests.

persistentETag Generate the persistent Citrix ADC specific ETag for the HTTP response with ETag header.

http2 Choose whether to enable support for HTTP/2.

http2Direct Choose whether to enable support for Direct HTTP/2.

http2StrictCipher Choose whether to enable strict HTTP/2 cipher selection

http2AltSvcFrame Choose whether to enable support for sending HTTP/2 ALTSVC frames. When enabled, the ADC sends HTTP/2 ALTSVC frames to HTTP/2 clients, instead of the Alt-Svc response header field. Not applicable to servers.

altsvc Choose whether to enable support for Alternative Services.

altSvcValue Configure a custom Alternative Services header value that should be inserted in the response to advertise a HTTP/SSL/HTTP_QUIC vserver.

http2MaxHeaderListSize Maximum size of header list that the Citrix ADC is prepared to accept, in bytes. NOTE: The actual plain text header size that the Citrix ADC accepts is limited by maxHeaderLen. Please change maxHeaderLen parameter as well when modifying http2MaxHeaderListSize.

http2MaxFrameSize Maximum size of the frame payload that the Citrix ADC is willing to receive, in bytes.

http2MaxConcurrentStreams Maximum number of concurrent streams that is allowed per connection.

http2InitialConnWindowSize Initial window size for connection level flow control, in bytes.

http2InitialWindowSize Initial window size for stream level flow control, in bytes.

http2HeaderTableSize Maximum size of the header compression table used to decode header blocks, in bytes.

http2MinSeverConn Minimum number of HTTP2 connections established to backend server, on receiving HTTP requests from client before multiplexing the streams into the available HTTP/2 connections.

http2MaxPingFramesPerMin Maximum number of ping frames allowed in HTTP2 connection per minute

http2MaxSettingsFramesPerMin Maximum number of settings frames allowed in HTTP2 connection per minute

http2MaxResetFramesPerMin Maximum number of reset frames allowed in HTTP/2 connection per minute

http2MaxEmptyFramesPerMin Maximum number of empty frames allowed in HTTP2 connection per minute

grpcHoldLimit Maximum size in bytes allowed to buffer gRPC packets till trailer is received

grpcHoldTimeout Maximum time in milliseconds allowed to buffer gRPC packets till trailer is received. The value should be in multiples of 100

grpcLengthDelimitation Set to DISABLED for gRPC without a length delimitation.

reusePoolTimeout Idle timeout (in seconds) for server connections in re-use pool. Connections in the re-use pool are flushed, if they remain idle for the configured timeout.

maxHeaderLen Number of bytes to be queued to look for complete header before returning error. If complete header is not obtained after queuing these many bytes, request will be marked as invalid and no L7 processing will be done for that TCP connection.

maxHeaderFieldLen Number of bytes allowed for header field for HTTP header. If number of bytes exceeds beyond configured value, then request will be marked invalid

rtspTunnel Allow RTSP tunnel in HTTP. Once application/x-rtsp-tunnelled is seen in Accept or Content-Type header, Citrix ADC does not process Layer 7 traffic on this connection.

minReUsePool Minimum limit on the number of connections, from the Citrix ADC to a particular server that are kept in the reuse pool. This setting is helpful for optimal memory utilization and for

reducing the idle connections to the server just after the peak time. Zero implies no limit on reuse pool size.

builtin Flag to determine if http profile is built-in or not

apdexSvrRespTimeThreshold This option sets the satisfactory threshold (T) for server response time in milliseconds to be used for APDEX calculations. This means a transaction responding in less than this threshold is considered satisfactory. Transaction responding between T and 4*T is considered tolerable. Any transaction responding in more than 4*T time is considered frustrating. Citrix ADC maintains stats for such tolerable and frustrating transcations. Server Response time related apdex counters are only updated on backend services or a backend vserver which is not accepting client traffic.

apdexCltRespTimeThreshold This option sets the satisfactory threshold (T) for client response time in milliseconds to be used for APDEX calculations. This means a transaction responding in less than this threshold is considered satisfactory. Transaction responding between T and 4*T is considered tolerable. Any transaction responding in more than 4*T time is considered frustrating. Citrix ADC maintains stats for such tolerable and frustrating transcations. And client response time related apdex counters are only updated on a vserver which receives clients traffic.

http3 Choose whether to enable support for HTTP/3.

http3MaxHeaderFieldSectionSize Maximum size of the HTTP/3 header field section, in bytes.

http3MaxHeaderTableSize Maximum size of the HTTP/3 QPACK dynamic header table, in bytes.

http3MaxHeaderBlockedStreams Maximum number of HTTP/3 streams that can be blocked while HTTP/3 headers are being decoded.

httppipelinebuffsize Application pipeline request buffering size, in bytes.

allowOnlyWordCharactersAndHyphen Allow only word character hyphen

dropInvalreqsWarning Display warning if Drop invalid reqs is disabled in the profile

passProtocolUpgrade Pass protocol upgrade request to the server.

feature The feature to be checked while applying this config

devno count

Example

show http profile

add ns httpProfile

Adds an HTTP profile to the Citrix ADC.

Synopsis

add ns httpProfile <name>

Arguments

name Name for an HTTP profile. Must begin with a letter, number, or the underscore \(_\) character. Other characters allowed, after the first character, are the hyphen \(-\), period \(.\), hash \(#\), space \(\), at \(@\), colon \(:\), and equal \(=\) characters. The name of a HTTP profile cannot be changed after it is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my http profile" or 'my http profile'\).

dropInvalReqs Drop invalid HTTP requests or responses.

Possible values: ENABLED, DISABLED Default value: DISABLED

markHttp09Inval Mark HTTP/0.9 requests as invalid.

Possible values: ENABLED, DISABLED Default value: DISABLED

markConnReqInval Mark CONNECT requests as invalid.

Possible values: ENABLED, DISABLED Default value: DISABLED

markTraceReqInval Mark TRACE requests as invalid.

Possible values: ENABLED, DISABLED Default value: DISABLED

markRfc7230NonCompliantInval Mark RFC7230 non-compliant transaction as invalid

Possible values: ENABLED, DISABLED Default value: DISABLED

markHTTPHeaderExtraWSError Mark Http header with extra white space as invalid

Possible values: ENABLED, DISABLED Default value: DISABLED

cmpOnPush Start data compression on receiving a TCP packet with PUSH flag set.

Possible values: ENABLED, DISABLED Default value: DISABLED

conMultiplex Reuse server connections for requests from more than one client connections.

Possible values: ENABLED, DISABLED Default value: ENABLED

maxReusePool Maximum limit on the number of connections, from the Citrix ADC to a particular server that are kept in the reuse pool. This setting is helpful for optimal memory utilization and for reducing the idle connections to the server just after the peak time. Zero implies no limit on reuse pool size. If non-zero value is given, it has to be greater than or equal to the number of running Packet Engines. Default value: 0 Minimum value: 0 Maximum value: 360000

dropExtraCRLF Drop any extra 'CR' and 'LF' characters present after the header.

Possible values: ENABLED, DISABLED Default value: ENABLED

incompHdrDelay Maximum time to wait, in milliseconds, between incomplete header packets. If the header packets take longer to arrive at Citrix ADC, the connection is silently dropped. Default value: 7000 Minimum value: 1 Maximum value: 360000

webSocket HTTP connection to be upgraded to a web socket connection. Once upgraded, Citrix ADC does not process Layer 7 traffic on this connection.

Possible values: ENABLED, DISABLED Default value: DISABLED

rtspTunnel Allow RTSP tunnel in HTTP. Once application/x-rtsp-tunnelled is seen in Accept or Content-Type header, Citrix ADC does not process Layer 7 traffic on this connection.

Possible values: ENABLED, DISABLED Default value: DISABLED

reqTimeout Time, in seconds, within which the HTTP request must complete. If the request does not complete within this time, the specified request timeout action is executed. Zero disables the timeout. Default value: 0 Minimum value: 0 Maximum value: 86400

adptTimeout Adapts the configured request timeout based on flow conditions. The timeout is increased or decreased internally and applied on the flow.

Possible values: ENABLED, DISABLED Default value: DISABLED

reqTimeoutAction Action to take when the HTTP request does not complete within the specified request timeout duration. You can configure the following actions:

- RESET - Send RST (reset) to client when timeout occurs.
- DROP - Drop silently when timeout occurs.
- Custom responder action - Name of the responder action to trigger when timeout occurs, used to send custom message.

dropExtraData Drop any extra data when server sends more data than the specified content-length.

Possible values: ENABLED, DISABLED Default value: DISABLED

webLog Enable or disable web logging.

Possible values: ENABLED, DISABLED Default value: ENABLED

clientIpHdrExpr Name of the header that contains the real client IP address.

maxReq Maximum number of requests allowed on a single connection. Zero implies no limit on the number of requests. Default value: 0 Minimum value: 0 Maximum value: 65534

persistentETag Generate the persistent Citrix ADC specific ETag for the HTTP response with ETag header.

Possible values: ENABLED, DISABLED Default value: DISABLED

http2 Choose whether to enable support for HTTP/2.

Possible values: ENABLED, DISABLED Default value: DISABLED

http2Direct Choose whether to enable support for Direct HTTP/2.

Possible values: ENABLED, DISABLED Default value: DISABLED

http2StrictCipher Choose whether to enable strict HTTP/2 cipher selection

Possible values: ENABLED, DISABLED Default value: ENABLED

http2AltSvcFrame Choose whether to enable support for sending HTTP/2 ALTSVC frames. When enabled, the ADC sends HTTP/2 ALTSVC frames to HTTP/2 clients, instead of the Alt-Svc response header field. Not applicable to servers.

Possible values: ENABLED, DISABLED Default value: DISABLED

altsvc Choose whether to enable support for Alternative Services.

Possible values: ENABLED, DISABLED Default value: DISABLED

altSvcValue Configure a custom Alternative Services header value that should be inserted in the response to advertise a HTTP/SSL/HTTP_QUIC vserver.

reusePoolTimeout Idle timeout (in seconds) for server connections in re-use pool. Connections in the re-use pool are flushed, if they remain idle for the configured timeout. Default value: 0 Minimum value: 0 Maximum value: 31536000

maxHeaderLen Number of bytes to be queued to look for complete header before returning error. If complete header is not obtained after queuing these many bytes, request will be marked as invalid and no L7 processing will be done for that TCP connection. Default value: 24820 Minimum value: 2048 Maximum value: 122880

maxHeaderFieldLen Number of bytes allowed for header field for HTTP header. If number of bytes exceeds beyond configured value, then request will be marked invalid Default value: 24820 Minimum value: 2048 Maximum value: 122880

minReUsePool Minimum limit on the number of connections, from the Citrix ADC to a particular server that are kept in the reuse pool. This setting is helpful for optimal memory utilization and for reducing the idle connections to the server just after the peak time. Zero implies no limit on reuse pool size. Default value: 0 Minimum value: 0 Maximum value: 360000

http2MaxHeaderListSize Maximum size of header list that the Citrix ADC is prepared to accept, in bytes. NOTE: The actual plain text header size that the Citrix ADC accepts is limited by maxHeaderLen. Please change maxHeaderLen parameter as well when modifying http2MaxHeaderListSize. Default value: 24576 Minimum value: 8192 Maximum value: 131071

http2MaxFrameSize Maximum size of the frame payload that the Citrix ADC is willing to receive, in bytes. Default value: 16384 Minimum value: 16384 Maximum value: 32768

http2MaxConcurrentStreams Maximum number of concurrent streams that is allowed per connection. Default value: 100 Minimum value: 0 Maximum value: 1000

http2InitialConnWindowSize Initial window size for connection level flow control, in bytes. Default value: 65535 Minimum value: 65535 Maximum value: 67108864

http2InitialWindowSize Initial window size for stream level flow control, in bytes. Default value: 65535 Minimum value: 8192 Maximum value: 20971520

http2HeaderTableSize Maximum size of the header compression table used to decode header blocks, in bytes. Default value: 4096 Minimum value: 0 Maximum value: 131072

http2MinSeverConn Minimum number of HTTP2 connections established to backend server, on receiving HTTP requests from client before multiplexing the streams into the available HTTP/2 connections. Default value: 20 Minimum value: 1 Maximum value: 360000

http2MaxPingFramesPerMin Maximum number of ping frames allowed in HTTP2 connection per minute Default value: 60 Minimum value: 1 Maximum value: 360000

http2MaxSettingsFramesPerMin Maximum number of settings frames allowed in HTTP2 connection per minute Default value: 15 Minimum value: 1 Maximum value: 360000

http2MaxResetFramesPerMin Maximum number of reset frames allowed in HTTP/2 connection per minute Default value: 90 Minimum value: 1 Maximum value: 360000

http2MaxEmptyFramesPerMin Maximum number of empty frames allowed in HTTP2 connection per minute Default value: 60 Minimum value: 1 Maximum value: 360000

grpcHoldLimit Maximum size in bytes allowed to buffer gRPC packets till trailer is received Default value: 131072 Minimum value: 0 Maximum value: 33554432

grpcHoldTimeout Maximum time in milliseconds allowed to buffer gRPC packets till trailer is received. The value should be in multiples of 100 Default value: 1000 Minimum value: 0 Maximum value: 180000

grpcLengthDelimitation Set to DISABLED for gRPC without a length delimitation.

Possible values: ENABLED, DISABLED Default value: ENABLED

apdexCltRespTimeThreshold This option sets the satisfactory threshold (T) for client response time in milliseconds to be used for APDEX calculations. This means a transaction responding in less than this threshold is considered satisfactory. Transaction responding between T and 4*T is considered tolerable. Any transaction responding in more than 4*T time is considered frustrating. Citrix ADC maintains stats for such tolerable and frustrating transcations. And client response time related apdex counters are only updated on a vserver which receives clients traffic. Default value: 500 Minimum value: 1 Maximum value: 3600000

http3 Choose whether to enable support for HTTP/3.

Possible values: ENABLED, DISABLED Default value: DISABLED

http3MaxHeaderFieldSectionSize Maximum size of the HTTP/3 header field section, in bytes. Default value: 24576 Minimum value: 8192 Maximum value: 131072

http3MaxHeaderTableSize Maximum size of the HTTP/3 QPACK dynamic header table, in bytes. Default value: 4096 Minimum value: 0 Maximum value: 131072

http3MaxHeaderBlockedStreams Maximum number of HTTP/3 streams that can be blocked while HTTP/3 headers are being decoded. Default value: 100 Minimum value: 1 Maximum value: 500

httppipelinebuffsize Application pipeline request buffering size, in bytes. Default value: 131072 Minimum value: 131072 Maximum value: 20971520

allowOnlyWordCharactersAndHyphen When enabled allows only the word characters and hyphen in the request/response header names and the connection will be reset for the other characters. When disabled allows any visible (printing) characters (%21-%7E) except delimiters (double quotes and "(),/:;<=>?@{}").

Possible values: ENABLED, DISABLED Default value: DISABLED

passProtocolUpgrade Pass protocol upgrade request to the server.

Possible values: ENABLED, DISABLED Default value: ENABLED

Example

add httpprofile <profile name> -dropInvalReqs ON -markHttp09Inval ON

set ns httpProfile

Modifies the attributes of an HTTP profile.

Synopsis

set ns httpProfile <name>

Arguments

name Name of the HTTP profile to be modified.

dropInvalReqs Drop invalid HTTP requests or responses.

Possible values: ENABLED, DISABLED Default value: DISABLED

markHttp09Inval Mark HTTP/0.9 requests as invalid.

Possible values: ENABLED, DISABLED Default value: DISABLED

markConnReqInval Mark CONNECT requests as invalid.

Possible values: ENABLED, DISABLED Default value: DISABLED

markTraceReqInval Mark TRACE requests as invalid.

Possible values: ENABLED, DISABLED Default value: DISABLED

markRfc7230NonCompliantInval Mark RFC7230 non-compliant transaction as invalid

Possible values: ENABLED, DISABLED Default value: DISABLED

markHTTPHeaderExtraWSError Mark Http header with extra white space as invalid

Possible values: ENABLED, DISABLED Default value: DISABLED

cmpOnPush Start data compression on receiving a TCP packet with PUSH flag set.

Possible values: ENABLED, DISABLED Default value: DISABLED

conMultiplex Reuse server connections for requests from more than one client connections.

Possible values: ENABLED, DISABLED Default value: ENABLED

maxReusePool Maximum limit on the number of connections, from the Citrix ADC to a particular server that are kept in the reuse pool. This setting is helpful for optimal memory utilization and for reducing the idle connections to the server just after the peak time. Zero implies no limit on reuse pool size. If non-zero value is given, it has to be greater than or equal to the number of running Packet Engines. Default value: 0 Minimum value: 0 Maximum value: 360000

dropExtraCRLF Drop any extra 'CR' and 'LF' characters present after the header.

Possible values: ENABLED, DISABLED Default value: ENABLED

incompHdrDelay Maximum time to wait, in milliseconds, between incomplete header packets. If the header packets take longer to arrive at Citrix ADC, the connection is silently dropped. Default value: 7000 Minimum value: 1 Maximum value: 360000

webSocket HTTP connection to be upgraded to a web socket connection. Once upgraded, Citrix ADC does not process Layer 7 traffic on this connection.

Possible values: ENABLED, DISABLED Default value: DISABLED

rtspTunnel Allow RTSP tunnel in HTTP. Once application/x-rtsp-tunnelled is seen in Accept or Content-Type header, Citrix ADC does not process Layer 7 traffic on this connection.

Possible values: ENABLED, DISABLED Default value: DISABLED

reqTimeout Time, in seconds, within which the HTTP request must complete. If the request does not complete within this time, the specified request timeout action is executed. Zero disables the timeout. Default value: 0 Minimum value: 0 Maximum value: 86400

adptTimeout Adapts the configured request timeout based on flow conditions. The timeout is increased or decreased internally and applied on the flow.

Possible values: ENABLED, DISABLED Default value: DISABLED

reqTimeoutAction Action to take when the HTTP request does not complete within the specified request timeout duration. You can configure the following actions:

- RESET - Send RST (reset) to client when timeout occurs.
- DROP - Drop silently when timeout occurs.
- Custom responder action - Name of the responder action to trigger when timeout occurs, used to send custom message.

dropExtraData Drop any extra data when server sends more data than the specified content-length.

Possible values: ENABLED, DISABLED Default value: DISABLED

webLog Enable or disable web logging.

Possible values: ENABLED, DISABLED Default value: ENABLED

clientIpHdrExpr Name of the header that contains the real client IP address.

maxReq Maximum number of requests allowed on a single connection. Zero implies no limit on the number of requests. Default value: 0 Minimum value: 0 Maximum value: 65534

persistentETag Generate the persistent Citrix ADC specific ETag for the HTTP response with ETag header.

Possible values: ENABLED, DISABLED Default value: DISABLED

http2 Choose whether to enable support for HTTP/2.

Possible values: ENABLED, DISABLED Default value: DISABLED

http2Direct Choose whether to enable support for Direct HTTP/2.

Possible values: ENABLED, DISABLED Default value: DISABLED

http2StrictCipher Choose whether to enable strict HTTP/2 cipher selection

Possible values: ENABLED, DISABLED Default value: ENABLED

http2AltSvcFrame Choose whether to enable support for sending HTTP/2 ALTSVC frames. When enabled, the ADC sends HTTP/2 ALTSVC frames to HTTP/2 clients, instead of the Alt-Svc response header field. Not applicable to servers.

Possible values: ENABLED, DISABLED Default value: DISABLED

altsvc Choose whether to enable support for Alternative Services.

Possible values: ENABLED, DISABLED Default value: DISABLED

altSvcValue Configure a custom Alternative Services header value that should be inserted in the response to advertise a HTTP/SSL/HTTP_QUIC vserver.

http2MaxHeaderListSize Maximum size of header list that the Citrix ADC is prepared to accept, in bytes. NOTE: The actual plain text header size that the Citrix ADC accepts is limited by maxHeaderLen. Please change maxHeaderLen parameter as well when modifying http2MaxHeaderListSize. Default value: 24576 Minimum value: 8192 Maximum value: 131071

http2MaxFrameSize Maximum size of the frame payload that the Citrix ADC is willing to receive, in bytes. Default value: 16384 Minimum value: 16384 Maximum value: 32768

http2MaxConcurrentStreams Maximum number of concurrent streams that is allowed per connection. Default value: 100 Minimum value: 0 Maximum value: 1000

http2InitialConnWindowSize Initial window size for connection level flow control, in bytes. Default value: 65535 Minimum value: 65535 Maximum value: 67108864

http2InitialWindowSize Initial window size for stream level flow control, in bytes. Default value: 65535 Minimum value: 8192 Maximum value: 20971520

http2HeaderTableSize Maximum size of the header compression table used to decode header blocks, in bytes. Default value: 4096 Minimum value: 0 Maximum value: 131072

http2MinSeverConn Minimum number of HTTP2 connections established to backend server, on receiving HTTP requests from client before multiplexing the streams into the available HTTP/2 connections. Default value: 20 Minimum value: 1 Maximum value: 360000

http2MaxPingFramesPerMin Maximum number of ping frames allowed in HTTP2 connection per minute Default value: 60 Minimum value: 1 Maximum value: 360000

http2MaxSettingsFramesPerMin Maximum number of settings frames allowed in HTTP2 connection per minute Default value: 15 Minimum value: 1 Maximum value: 360000

http2MaxResetFramesPerMin Maximum number of reset frames allowed in HTTP/2 connection per minute Default value: 90 Minimum value: 1 Maximum value: 360000

http2MaxEmptyFramesPerMin Maximum number of empty frames allowed in HTTP2 connection per minute Default value: 60 Minimum value: 1 Maximum value: 360000

grpcHoldLimit Maximum size in bytes allowed to buffer gRPC packets till trailer is received Default value: 131072 Minimum value: 0 Maximum value: 33554432

grpcHoldTimeout Maximum time in milliseconds allowed to buffer gRPC packets till trailer is received. The value should be in multiples of 100 Default value: 1000 Minimum value: 0 Maximum value: 180000

grpcLengthDelimitation Set to DISABLED for gRPC without a length delimitation.

Possible values: ENABLED, DISABLED Default value: ENABLED

reusePoolTimeout Idle timeout (in seconds) for server connections in re-use pool. Connections in the re-use pool are flushed, if they remain idle for the configured timeout. Default value: 0 Minimum value: 0 Maximum value: 31536000

maxHeaderLen Number of bytes to be queued to look for complete header before returning error. If complete header is not obtained after queuing these many bytes, request will be marked as invalid and no L7 processing will be done for that TCP connection. Default value: 24820 Minimum value: 2048 Maximum value: 122880

maxHeaderFieldLen Number of bytes allowed for header field for HTTP header. If number of bytes exceeds beyond configured value, then request will be marked invalid Default value: 24820 Minimum value: 2048 Maximum value: 122880

minReUsePool Minimum limit on the number of connections, from the Citrix ADC to a particular server that are kept in the reuse pool. This setting is helpful for optimal memory utilization and for reducing the idle connections to the server just after the peak time. Zero implies no limit on reuse pool size. Default value: 0 Minimum value: 0 Maximum value: 360000

apdexCltRespTimeThreshold This option sets the satisfactory threshold (T) for client response time in milliseconds to be used for APDEX calculations. This means a transaction responding in less than this threshold is considered satisfactory. Transaction responding between T and 4*T is considered tolerable. Any transaction responding in more than 4*T time is considered frustrating.

Citrix ADC maintains stats for such tolerable and frustrating transcations. And client response time related apdex counters are only updated on a vserver which receives clients traffic. Default value: 500 Minimum value: 1 Maximum value: 3600000

http3 Choose whether to enable support for HTTP/3.

Possible values: ENABLED, DISABLED Default value: DISABLED

http3MaxHeaderFieldSectionSize Maximum size of the HTTP/3 header field section, in bytes. Default value: 24576 Minimum value: 8192 Maximum value: 131072

http3MaxHeaderTableSize Maximum size of the HTTP/3 QPACK dynamic header table, in bytes. Default value: 4096 Minimum value: 0 Maximum value: 131072

http3MaxHeaderBlockedStreams Maximum number of HTTP/3 streams that can be blocked while HTTP/3 headers are being decoded. Default value: 100 Minimum value: 1 Maximum value: 500

httppipelinebuffsize Application pipeline request buffering size, in bytes. Default value: 131072 Minimum value: 131072 Maximum value: 20971520

allowOnlyWordCharactersAndHyphen When enabled allows only the word characters and hyphen in the request/response header names and the connection will be reset for the other characters. When disabled allows any visible (printing) characters (%21-%7E) except delimiters (double quotes and "(),/:;<=>?@{}").

Possible values: ENABLED, DISABLED Default value: DISABLED

passProtocolUpgrade Pass protocol upgrade request to the server.

Possible values: ENABLED, DISABLED Default value: ENABLED

Example

set httpprofile <profile name> -dropInvalReqs ON -markHttp09Inval ON

rm ns httpProfile

Removes an HTTP profile from the appliance.

Synopsis

rm ns httpProfile <name>

Arguments

name Name of the HTTP profile to be removed.

Example

rm httpprofile <profile name>

unset ns httpProfile

Removes the attributes of the HTTP profile. Attributes for which a default value is available revert to their default values. Refer to the 'set ns httpProfile' command for a description of the parameters..Refer to the set ns httpProfile command for meanings of the arguments.

Synopsis

unset ns httpProfile <name>

ns-icapProfile

The following operations can be performed on "ns-icapProfile":

unset| set| show| rm| add|

unset ns icapProfile

Use this command to remove ns icapProfile settings.Refer to the set ns icapProfile command for meanings of the arguments.

Synopsis

unset ns icapProfile <name>

set ns icapProfile

Modifies the attributes of an ICAP profile

Synopsis

set ns icapProfile <name>

Arguments

name Name for an ICAP profile. Must begin with a letter, number, or the underscore \(_\) character. Other characters allowed, after the first character, are the hyphen \(-\), period \(.\), hash \(#\), space

\(\), at \(@\), colon \(:\), and equal \(=\) characters. The name of a ICAP profile cannot be changed after it is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my icap profile" or 'my icap profile'\).

preview Enable or Disable preview header with ICAP request. This feature allows an ICAP server to see the beginning of a transaction, then decide if it wants to opt-out of the transaction early instead of receiving the remainder of the request message.

Possible values: ENABLED, DISABLED Default value: DISABLED

previewLength Value of Preview Header field. Citrix ADC uses the minimum of this set value and the preview size received on OPTIONS response. Default value: 4096 Minimum value: 0 Maximum value: 4294967294

uri URI representing icap service. It is a mandatory argument while creating an icapprofile.

hostHeader ICAP Host Header

userAgent ICAP User Agent Header String

Mode ICAP Mode of operation. It is a mandatory argument while creating an icapprofile.

Possible values: REQMOD, RESPMOD

queryParams Query parameters to be included with ICAP request URI. Entered values should be in arg=value format. For more than one parameters, add & separated values. e.g.: arg1=val1&arg2=val2.

connectionKeepAlive If enabled, Citrix ADC keeps the ICAP connection alive after a transaction to reuse it to send next ICAP request.

Possible values: ENABLED, DISABLED Default value: ENABLED

allow204 Enable or Disable sending Allow: 204 header in ICAP request.

Possible values: ENABLED, DISABLED Default value: ENABLED

insertICAPHeaders Insert custom ICAP headers in the ICAP request to send to ICAP server. The headers can be static or can be dynamically constructed using PI Policy Expression. For example, to send static user agent and Client's IP address, the expression can be specified as "User-Agent: NS-ICAP-Client/V1.0\r\nX-Client-IP: "+CLIENT.IP.SRC+"\r\n". The Citrix ADC does not check the

validity of the specified header name-value. You must manually validate the specified header syntax.

insertHTTPRequest Exact HTTP request, in the form of an expression, which the Citrix ADC encapsulates and sends to the ICAP server. If you set this parameter, the ICAP request is sent using only this header. This can be used when the HTTP header is not available to send or ICAP server only needs part of the incoming HTTP request. The request expression is constrained by the feature for which it is used. The Citrix ADC does not check the validity of this request. You must manually validate the request.

reqTimeout Time, in seconds, within which the remote server should respond to the ICAP-request. If the Netscaler does not receive full response with this time, the specified request timeout action is performed. Zero value disables this timeout functionality. Default value: 0 Minimum value: 0 Maximum value: 86400

reqTimeoutAction Name of the action to perform if the Vserver/Server representing the remote service does not respond with any response within the timeout value configured. The Supported actions are

- BYPASS - This Ignores the remote server response and sends the request/response to Client/ Server.
    - If the ICAP response with Encapsulated headers is not received within the request-timeout value configured, this Ignores the remote ICAP server response and sends the Full request/ response to Server/Client.
- RESET - Reset the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend the request if desired.
- DROP - Drop the request without sending a response to the user.

Possible values: BYPASS, DROP, RESET Default value: RESET

logAction Name of the audit message action which would be evaluated on receiving the ICAP response to emit the logs.

Example

set icapprofile <profile-name> -preview ENABLED -previewLength 5066

show ns icapProfile

Displays ICAP profile/s configured on Citrix ADC

Synopsis

show ns icapProfile

Arguments

name Name of the ICAP profile to be displayed

Output

preview Enable or Disable preview header with ICAP request. This feature allows an ICAP server to see the beginning of a transaction, then decide if it wants to opt-out of the transaction early instead of receiving the remainder of the request message.

previewLength Value of Preview Header field. Citrix ADC uses the minimum of this set value and the preview size received on OPTIONS response.

uri URI representing icap service. It is a mandatory argument while creating an icapprofile.

hostHeader ICAP Host Header

userAgent ICAP User Agent Header String

Mode ICAP Mode of operation. It is a mandatory argument while creating an icapprofile.

queryParams Query parameters to be included with ICAP request URI. Entered values should be in arg=value format. For more than one parameters, add & separated values. e.g.: arg1=val1&arg2=val2.

connectionKeepAlive If enabled, Citrix ADC keeps the ICAP connection alive after a transaction to reuse it to send next ICAP request.

allow204 Enable or Disable sending Allow: 204 header in ICAP request.

insertICAPHeaders Insert custom ICAP headers in the ICAP request to send to ICAP server. The headers can be static or can be dynamically constructed using PI Policy Expression. For example, to send static user agent and Client's IP address, the expression can be specified as "User-Agent: NS-ICAP-Client/V1.0\r\nX-Client-IP: "+CLIENT.IP.SRC+"\r\n". The Citrix ADC does not check the validity of the specified header name-value. You must manually validate the specified header syntax.

insertHTTPRequest Exact HTTP request, in the form of an expression, which the Citrix ADC encapsulates and sends to the ICAP server. If you set this parameter, the ICAP request is sent using only this header. This can be used when the HTTP header is not available to send or ICAP

server only needs part of the incoming HTTP request. The request expression is constrained by the feature for which it is used. The Citrix ADC does not check the validity of this request. You must manually validate the request.

reqTimeout Time, in seconds, within which the remote server should respond to the ICAP-request. If the Netscaler does not receive full response with this time, the specified request timeout action is performed. Zero value disables this timeout functionality.

reqTimeoutAction Name of the action to perform if the Vserver/Server representing the remote service does not respond with any response within the timeout value configured. The Supported actions are

- BYPASS - This Ignores the remote server response and sends the request/response to Client/ Server.
    - If the ICAP response with Encapsulated headers is not received within the request-timeout value configured, this Ignores the remote ICAP server response and sends the Full request/ response to Server/Client.
- RESET - Reset the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend the request if desired.
- DROP - Drop the request without sending a response to the user.

logAction Name of the audit message action which would be evaluated on receiving the ICAP response to emit the logs.

devno count stateflag

Example

show icapprofile

rm ns icapProfile

Removes an ICAP profile.

Synopsis

rm ns icapProfile <name>

Arguments

name Name of the ICAP profile to be removed

Example

rm icapprofile <profile-name>

add ns icapProfile

Adds an ICAP profile to the Citrix ADC.

Synopsis

add ns icapProfile <name> -uri <string> -Mode (REQMOD | RESPMOD)

Arguments

name Name for an ICAP profile. Must begin with a letter, number, or the underscore \(_\) character. Other characters allowed, after the first character, are the hyphen \(-\), period \(.\), hash \(#\), space \(\), at \(@\), colon \(:\), and equal \(=\) characters. The name of a ICAP profile cannot be changed after it is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my icap profile" or 'my icap profile'\).

preview Enable or Disable preview header with ICAP request. This feature allows an ICAP server to see the beginning of a transaction, then decide if it wants to opt-out of the transaction early instead of receiving the remainder of the request message.

Possible values: ENABLED, DISABLED Default value: DISABLED

previewLength Value of Preview Header field. Citrix ADC uses the minimum of this set value and the preview size received on OPTIONS response. Default value: 4096 Minimum value: 0 Maximum value: 4294967294

uri URI representing icap service. It is a mandatory argument while creating an icapprofile.

hostHeader ICAP Host Header

userAgent ICAP User Agent Header String

Mode ICAP Mode of operation. It is a mandatory argument while creating an icapprofile.

Possible values: REQMOD, RESPMOD

queryParams Query parameters to be included with ICAP request URI. Entered values should be in arg=value format. For more than one parameters, add & separated values. e.g.: arg1=val1&arg2=val2.

connectionKeepAlive If enabled, Citrix ADC keeps the ICAP connection alive after a transaction to reuse it to send next ICAP request.

Possible values: ENABLED, DISABLED Default value: ENABLED

allow204 Enable or Disable sending Allow: 204 header in ICAP request.

Possible values: ENABLED, DISABLED Default value: ENABLED

insertICAPHeaders Insert custom ICAP headers in the ICAP request to send to ICAP server. The headers can be static or can be dynamically constructed using PI Policy Expression. For example, to send static user agent and Client's IP address, the expression can be specified as "User-Agent: NS-ICAP-Client/V1.0\r\nX-Client-IP: "+CLIENT.IP.SRC+"\r\n". The Citrix ADC does not check the validity of the specified header name-value. You must manually validate the specified header syntax.

insertHTTPRequest Exact HTTP request, in the form of an expression, which the Citrix ADC encapsulates and sends to the ICAP server. If you set this parameter, the ICAP request is sent using only this header. This can be used when the HTTP header is not available to send or ICAP server only needs part of the incoming HTTP request. The request expression is constrained by the feature for which it is used. The Citrix ADC does not check the validity of this request. You must manually validate the request.

reqTimeout Time, in seconds, within which the remote server should respond to the ICAP-request. If the Netscaler does not receive full response with this time, the specified request timeout action is performed. Zero value disables this timeout functionality. Default value: 0 Minimum value: 0 Maximum value: 86400

reqTimeoutAction Name of the action to perform if the Vserver/Server representing the remote service does not respond with any response within the timeout value configured. The Supported actions are

- BYPASS - This Ignores the remote server response and sends the request/response to Client/ Server.
    - If the ICAP response with Encapsulated headers is not received within the request-timeout value configured, this Ignores the remote ICAP server response and sends the Full request/ response to Server/Client.
- RESET - Reset the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend the request if desired.

- DROP - Drop the request without sending a response to the user.

Possible values: BYPASS, DROP, RESET Default value: RESET

logAction Name of the audit message action which would be evaluated on receiving the ICAP response to emit the logs.

Example

add icapprofile reqmod-profile-previewLen 1024-URI"/req_scan" -HostHeader"Webroot.reqsca" -UserAgen"NS SWG Proxy"

ns-idletimeout

The following operations can be performed on "ns-idletimeout":

unset| set| show|

unset ns idletimeout

Use this command to remove ns idletimeout settings.Refer to the set ns idletimeout command for meanings of the arguments.NOTE: This command is deprecated.

Synopsis

set ns idletimeout

Set the pcb/natpcb idletimeout. NOTE: This command is deprecated.

Synopsis

Arguments

tcpsvr Set the idletimeout for server side pcb.

tcpclt Set the idletimeout for client side pcb.

nontcpsvrclt Set the idletimeout for natpcb. Default value: 120 Minimum value: 1

Example

set ns idletimeout -tcpsvr 120 set ns idletimeout -tcpclt 120 set ns idletimeout -nontcpsvrclt 120

show ns idletimeout

Display the global setting of pcb/natpcb idletimeout. NOTE: This command is deprecated.This command is deprecated in favour of 'set ns timeout'

Synopsis

Arguments

Output

tcpsvr Set the idletimeout for server side pcb.

tcpclt Set the idletimeout for client side pcb.

nontcpsvrclt Set the idletimeout for natpcb.

ns-info

The following operations can be performed on "ns-info":

show ns info

Displays the following details of the Citrix ADC:

- Software version
- Citrix ADC IP address and subnet mask
- Number of mapped IP addresses
- Identifies the appliance as a standalone appliance, a part of an HA pair, or is a cluster node
- Current time on the system and timestamp when the appliance was last updated
- Features that are enabled or disabled
- Modes that are enabled or disabled

Synopsis

show ns info

Example

An example of this command's output is shown below: System Rainier: Build 24, Date: Apr 25 2002, 21:13:25 System IP: 10.101.4.22 (mask: 255.255.0.0) Mapped IP: 10.101.4.23 Node: Standalone HTTP port(s): (none) Max connections: 0 Max requests per connection: 0 Client IP

insertion enabled: NO Cookie version: 0 Feature status: Web Logging: ON Surge Protection: ON Load Balancing: ON Content Switching: ON Cache Redirection: ON

Compression Control: OFF Priority Queuing: ON SSL Offloading: ON Global Server Load Balancing: ON N+1: OFF Dynamic Routing: OFF Content Filtering: ON Internal Caching: ON SSL VPN: OFF Mode status: Fast Ramp: ON Layer 2 mode: ON Use Source IP: OFF Client Keep-alive: ON TCP Buffering: OFF MAC-based forwarding: ON Edge configuration: OFF Use Subnet IP: OFF Layer 3 mode (ip forwarding): ON

ns-ip

The following operations can be performed on "ns-ip":

disable| rm| add| enable| unset| show| set|

disable ns ip

Disables the specified VIP address configured on the Citrix ADC.

Synopsis

disable ns ip (<IPAddress>@)

Arguments

IPAddress IP address that you want to disable.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. TD id 4095 is used reserved for LSN use Minimum value: 0 Maximum value: 4095

Example

disable ns ip 10.10.10.10

rm ns ip

Removes an IPv4 address configured on the Citrix ADC.

Synopsis

rm ns ip <IPAddress>@

Arguments

IPAddress IPv4 address that you want to remove.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. TD id 4095 is used reserved for LSN use Minimum value: 0 Maximum value: 4095

Example

rm ns ip 10.102.4.123

add ns ip

Creates an IPv4 address on the Citrix ADC.

Synopsis

add ns ip <IPAddress>@ <netmask> [-type <type> [-hostRoute (ENABLED | DISABLED) [-ospfLSAType (TYPE1 | TYPE5)]]]

Arguments

IPAddress IPv4 address to create on the Citrix ADC. Cannot be changed after the IP address is created.

netmask Subnet mask associated with the IP address.

type Type of the IP address to create on the Citrix ADC. Cannot be changed after the IP address is created. The following are the different types of Citrix ADC owned IP addresses:

- A Subnet IP (SNIP) address is used by the Citrix ADC to communicate with the servers. The Citrix ADC also uses the subnet IP address when generating its own packets, such as packets related to dynamic routing protocols, or to send monitor probes to check the health of the servers.
- A Virtual IP (VIP) address is the IP address associated with a virtual server. It is the IP address to which clients connect. An appliance managing a wide range of traffic may have many VIPs configured. Some of the attributes of the VIP address are customized to meet the requirements of the virtual server.
- A GSLB site IP (GSLBIP) address is associated with a GSLB site. It is not mandatory to specify a GSLBIP address when you initially configure the Citrix ADC. A GSLBIP address is used only when you create a GSLB site.

- A Cluster IP (CLIP) address is the management address of the cluster. All cluster configurations must be performed by accessing the cluster through this IP address.

Possible values: SNIP, VIP, NSIP, HostIP, GSLBsiteIP, CLIP Default value: SNIP

arp Respond to ARP requests for this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

icmp Respond to ICMP requests for this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

vServer Use this option to set (enable or disable) the virtual server attribute for this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

telnet Allow Telnet access to this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

ftp Allow File Transfer Protocol (FTP) access to this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

gui Allow graphical user interface (GUI) access to this IP address.

Possible values: ENABLED, SECUREONLY, DISABLED Default value: ENABLED

ssh Allow secure shell (SSH) access to this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

snmp Allow Simple Network Management Protocol (SNMP) access to this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

mgmtAccess Allow access to management applications on this IP address.

Possible values: ENABLED, DISABLED Default value: DISABLED

restrictAccess Block access to nonmanagement applications on this IP. This option is applicable for MIPs, SNIPs, and NSIP, and is disabled by default. Nonmanagement applications can run on the underlying Citrix ADC Free BSD operating system.

Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicRouting Allow dynamic routing on this IP address. Specific to Subnet IP (SNIP) address.

Possible values: ENABLED, DISABLED Default value: DISABLED

decrementTTL Decrement TTL by 1 when ENABLED.This setting is applicable only for UDP traffic.

Possible values: ENABLED, DISABLED Default value: DISABLED

hostRoute Option to push the VIP to ZebOS routing table for Kernel route redistribution through dynamic routing protocols

Possible values: ENABLED, DISABLED

advertiseOnDefaultPartition Advertise VIPs from Shared VLAN on Default Partition.

Possible values: ENABLED, DISABLED Default value: DISABLED

networkRoute Option to push the SNIP subnet to ZebOS routing table for Kernel route redistribution through dynamic routing protocol.

Possible values: ENABLED, DISABLED

tag Tag value for the network/host route associated with this IP. Default value: 0 Minimum value: 0

hostRtGw IP address of the gateway of the route for this VIP address. Default value: -1

metric Integer value to add to or subtract from the cost of the route advertised for the VIP address. Minimum value: -16777215

vserverRHILevel Advertise the route for the Virtual IP (VIP) address on the basis of the state of the virtual servers associated with that VIP.

- NONE - Advertise the route for the VIP address, regardless of the state of the virtual servers associated with the address.
- ONE VSERVER - Advertise the route for the VIP address if at least one of the associated virtual servers is in UP state.
- ALL VSERVER - Advertise the route for the VIP address if all of the associated virtual servers are in UP state.
- VSVR_CNTRLD - Advertise the route for the VIP address according to the RHIstate (RHI STATE) parameter setting on all the associated virtual servers of the VIP address along with their states.

When Vserver RHI Level (RHI) parameter is set to VSVR_CNTRLD, the following are different RHI behaviors for the VIP address on the basis of RHIstate (RHI STATE) settings on the virtual servers associated with the VIP address:

- If you set RHI STATE to PASSIVE on all virtual servers, the Citrix ADC always advertises the route for the VIP address.
- If you set RHI STATE to ACTIVE on all virtual servers, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers is in UP state. *If you set RHI STATE to ACTIVE on some and PASSIVE on others, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers, whose RHI STATE set to ACTIVE, is in UP state.

Possible values: ONE_VSERVER, ALL_VSERVERS, NONE, VSVR_CNTRLD Default value: ONE_VSERVER

ospfLSAType Type of LSAs to be used by the OSPF protocol, running on the Citrix ADC, for advertising the route for this VIP address.

Possible values: TYPE1, TYPE5 Default value: TYPE5

ospfArea ID of the area in which the type1 link-state advertisements (LSAs) are to be advertised for this virtual IP (VIP) address by the OSPF protocol running on the Citrix ADC. When this parameter is not set, the VIP is advertised on all areas. Default value: -1 Minimum value: 0 Maximum value: 4294967294LU

state Enable or disable the IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

vrID A positive integer that uniquely identifies a VMAC address for binding to this VIP address. This binding is used to set up Citrix ADCs in an active-active configuration using VRRP. Minimum value: 1 Maximum value: 255

icmpResponse Respond to ICMP requests for a Virtual IP (VIP) address on the basis of the states of the virtual servers associated with that VIP. Available settings function as follows:

- NONE - The Citrix ADC responds to any ICMP request for the VIP address, irrespective of the states of the virtual servers associated with the address.
- ONE VSERVER - The Citrix ADC responds to any ICMP request for the VIP address if at least one of the associated virtual servers is in UP state.

- ALL VSERVER - The Citrix ADC responds to any ICMP request for the VIP address if all of the associated virtual servers are in UP state.
- VSVR_CNTRLD - The behavior depends on the ICMP VSERVER RESPONSE setting on all the associated virtual servers.

The following settings can be made for the ICMP VSERVER RESPONSE parameter on a virtual server:

- If you set ICMP VSERVER RESPONSE to PASSIVE on all virtual servers, Citrix ADC always responds.
- If you set ICMP VSERVER RESPONSE to ACTIVE on all virtual servers, Citrix ADC responds if even one virtual server is UP.
- When you set ICMP VSERVER RESPONSE to ACTIVE on some and PASSIVE on others, Citrix ADC responds if even one virtual server set to ACTIVE is UP.

Possible values: NONE, ONE_VSERVER, ALL_VSERVERS, VSVR_CNTRLD Default value: 5

ownerNode The owner node in a Cluster for this IP address. Owner node can vary from 0 to 31. If ownernode is not specified then the IP is treated as Striped IP. Default value: 255 Minimum value: 0

arpResponse Respond to ARP requests for a Virtual IP (VIP) address on the basis of the states of the virtual servers associated with that VIP. Available settings function as follows:

- NONE - The Citrix ADC responds to any ARP request for the VIP address, irrespective of the states of the virtual servers associated with the address.
- ONE VSERVER - The Citrix ADC responds to any ARP request for the VIP address if at least one of the associated virtual servers is in UP state.
- ALL VSERVER - The Citrix ADC responds to any ARP request for the VIP address if all of the associated virtual servers are in UP state.

Possible values: NONE, ONE_VSERVER, ALL_VSERVERS Default value: 5

ownerDownResponse in cluster system, if the owner node is down, whether should it respond to icmp/arp

Possible values: YES, NO Default value: YES

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. TD id 4095 is used reserved for LSN use Minimum value: 0 Maximum value: 4095

arpOwner The arp owner in a Cluster for this IP address. It can vary from 0 to 31. Default value: 255 Minimum value: 0

mptcpAdvertise If enabled, this IP will be advertised by Citrix ADC to MPTCP enabled clients as part of ADD_ADDR option.

Possible values: YES, NO Default value: NO

Example

add ns ip 10.102.4.123 255.255.255.0

enable ns ip

Enables the specified VIP address configured on the Citrix ADC.

Synopsis

enable ns ip (<IPAddress>@)

Arguments

IPAddress IP address that you want to enable.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. TD id 4095 is used reserved for LSN use Minimum value: 0 Maximum value: 4095

Example

enable ns ip 10.10.10.10

unset ns ip

Modifies the parameters of an IPv4 address configured on the Citrix ADC..Refer to the set ns ip command for meanings of the arguments.

Synopsis

unset ns ip <IPAddress>@

Example

unset ns ip 10.102.4.123 -ospfArea

show ns ip

Displays settings of all the IPv4 addresses or of the specified IPv4 address configured on the Citrix ADC. To display settings of all the IPv4 addresses, run the command without any parameters. To display settings of a particular IPv4 address, specify the IPv4 address.

Synopsis

show ns ip [<IPAddress>]

Arguments

IPAddress IPv4 address whose details you want the Citrix ADC to display.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. TD id 4095 is used reserved for LSN use Minimum value: 0 Maximum value: 4095

type Display the settings of all IPv4 addresses of a particular type.

Possible values: SNIP, VIP, NSIP, HostIP, GSLBsiteIP, CLIP Default value: 0

Output

netmask The netmask of this IP.

flags The flags for this entry.

ipAttribute arp Whether arp is enabled or disabled.

icmp Whether icmp is enabled or disabled.

vServer Whether vserver is enabled or disabled.

telnet Whether telnet is enabled or disabled.

ssh Whether ssh is enabled or disabled.

gui Whether gui is (enabled|SecureOnly|disabled).

snmp Whether snmp is enabled or disabled.

ftp Whether ftp is enabled or disabled.

mgmtAccess Whether management access is enabled or disabled.

restrictAccess Blocking of all ports not used for management access enabled or disabled

decrementTTL Decrement TTL by 1 when ENABLED.This setting is applicable only for UDP traffic.

dynamicRouting Whether dynamic routing is enabled or disabled.

bgp Whether bgp is enabled or disabled.

ospf Whether ospf is enabled or disabled.

rip Whether rip is enabled or disabled.

hostRoute Option to push the VIP to ZebOS routing table for Kernel route redistribution through dynamic routing protocols

advertiseOnDefaultPartition Whether advertisment of VIPs of Shared VLAN is enabled or disabled.

networkRoute Option to push the SNIP subnet to ZebOS routing table for Kernel route redistribution through dynamic routing protocol.

tag Tag value for the network/host route associated with this IP.

hostRtGw Gateway used for advertising host route.

hostRtGwAct Actual Gateway used for advertising host route.

metric The metric value added or subtracted from the cost of the route.

ospfArea The area ID of the area in which OSPF Type1 LSAs are advertised. When ospfArea if not set, LSAs are advertised on all areas.

ospfAreaval The area ID of the area in which OSPF Type1 LSAs are advertised.

vserverRHILevel The rhi level for this IP.

VIPrtadv2BSD Whether this route is advertised to FreeBSD

VIPvserCount Number of vservers bound to this VIP

VIPvserDownCount Number of vservers bound to this VIP, which are down

VIPvsrvrRHIActiveCount Number of vservers that have RHI state ACTIVE

VIPvsrvrRHIActiveUpCount Number of vservers that have RHI state ACTIVE, which are UP

ospfLSAType The ospf lsa type to use while advertising this IP.

state Whether this ip is enabled or disabled.

freePorts Number of free Ports available on this IP

vrID A positive integer that uniquely identifies a VMAC address for binding to this VIP address. This binding is used to set up Citrix ADCs in an active-active configuration using VRRP.

ipType icmpResponse Respond to ICMP requests for a Virtual IP (VIP) address on the basis of the states of the virtual servers associated with that VIP. Available settings function as follows:

- NONE - The Citrix ADC responds to any ICMP request for the VIP address, irrespective of the states of the virtual servers associated with the address.
- ONE VSERVER - The Citrix ADC responds to any ICMP request for the VIP address if at least one of the associated virtual servers is in UP state.
- ALL VSERVER - The Citrix ADC responds to any ICMP request for the VIP address if all of the associated virtual servers are in UP state.
- VSVR_CNTRLD - The behavior depends on the ICMP VSERVER RESPONSE setting on all the associated virtual servers.

The following settings can be made for the ICMP VSERVER RESPONSE parameter on a virtual server:

- If you set ICMP VSERVER RESPONSE to PASSIVE on all virtual servers, Citrix ADC always responds.
- If you set ICMP VSERVER RESPONSE to ACTIVE on all virtual servers, Citrix ADC responds if even one virtual server is UP.
- When you set ICMP VSERVER RESPONSE to ACTIVE on some and PASSIVE on others, Citrix ADC responds if even one virtual server set to ACTIVE is UP.

ownerNode The owner node in a Cluster for this IP address. Owner node can vary from 0 to 31. If ownernode is not specified then the IP is treated as Striped IP.

arpResponse Respond to ARP requests for a Virtual IP (VIP) address on the basis of the states of the virtual servers associated with that VIP. Available settings function as follows:

- NONE - The Citrix ADC responds to any ARP request for the VIP address, irrespective of the states of the virtual servers associated with the address.

- ONE VSERVER - The Citrix ADC responds to any ARP request for the VIP address if at least one of the associated virtual servers is in UP state.
- ALL VSERVER - The Citrix ADC responds to any ARP request for the VIP address if all of the associated virtual servers are in UP state.

stateflag ownerDownResponse in cluster system, if the owner node is down, whether should it respond to icmp/arp

cfgflags This contains the flags for IP in DB

ipRefcount Used to keep reference count of IP

arpOwner The arp owner in a Cluster for this IP address. It can vary from 0 to 31.

operationalarpOwner Run time operational Arp Owner

mptcpAdvertise If enabled, this IP will be advertised by Citrix ADC to MPTCP enabled clients as part of ADD_ADDR option.

devno count

Example

show ns ip Ipaddress Type Mode Arp Icmp Vserver State Owner

1)10.102.169.16 Cluster IP Active Enabled Enabled NA Enabled Configuration Coordinator 2)10.102.169.18 NetScaler IP Active Enabled Enabled NA Enabled 1 3)10.102.169.19 NetScaler IP Active Enabled Enabled NA Enabled 2 4)10.102.169.17 VIP Active Enabled Enabled Enabled Enabled ALL

set ns ip

Modifies the parameters of an IPv4 address configured on the Citrix ADC.

Synopsis

set ns ip (<IPAddress>@) [-ospfLSAType (TYPE1 | TYPE5)]

Arguments

IPAddress IPv4 address whose parameters you want to modify.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. TD id 4095 is used reserved for LSN use Minimum value: 0 Maximum value: 4095

netmask Subnet mask associated with the IP address.

arp Respond to ARP requests for this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

icmp Respond to ICMP requests for this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

vServer Use this option to set (enable or disable) the virtual server attribute for this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

telnet Allow Telnet access to this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

ftp Allow File Transfer Protocol (FTP) access to this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

gui Allow graphical user interface (GUI) access to this IP address.

Possible values: ENABLED, SECUREONLY, DISABLED Default value: ENABLED

ssh Allow secure shell (SSH) access to this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

snmp Allow Simple Network Management Protocol (SNMP) access to this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

mgmtAccess Allow access to management applications on this IP address.

Possible values: ENABLED, DISABLED Default value: DISABLED

restrictAccess Block access to nonmanagement applications on this IP. This option is applicable for MIPs, SNIPs, and NSIP, and is disabled by default. Nonmanagement applications can run on the underlying Citrix ADC Free BSD operating system.

Possible values: ENABLED, DISABLED Default value: DISABLED

decrementTTL Decrement TTL by 1 when ENABLED.This setting is applicable only for UDP traffic.

Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicRouting Allow dynamic routing on this IP address. Specific to Subnet IP (SNIP) address.

Possible values: ENABLED, DISABLED Default value: DISABLED

hostRoute Option to push the VIP to ZebOS routing table for Kernel route redistribution through dynamic routing protocols

Possible values: ENABLED, DISABLED

advertiseOnDefaultPartition Advertise VIPs from Shared VLAN on Default Partition.

Possible values: ENABLED, DISABLED Default value: DISABLED

networkRoute Option to push the SNIP subnet to ZebOS routing table for Kernel route redistribution through dynamic routing protocol.

Possible values: ENABLED, DISABLED

hostRtGw IP address of the gateway of the route for this VIP address. Default value: -1

metric Integer value to add to or subtract from the cost of the route advertised for the VIP address. Minimum value: -16777215

vserverRHILevel Advertise the route for the Virtual IP (VIP) address on the basis of the state of the virtual servers associated with that VIP.

- NONE - Advertise the route for the VIP address, regardless of the state of the virtual servers associated with the address.
- ONE VSERVER - Advertise the route for the VIP address if at least one of the associated virtual servers is in UP state.
- ALL VSERVER - Advertise the route for the VIP address if all of the associated virtual servers are in UP state.
- VSVR_CNTRLD - Advertise the route for the VIP address according to the RHIstate (RHI STATE) parameter setting on all the associated virtual servers of the VIP address along with their states.

When Vserver RHI Level (RHI) parameter is set to VSVR_CNTRLD, the following are different RHI behaviors for the VIP address on the basis of RHIstate (RHI STATE) settings on the virtual servers associated with the VIP address:

- If you set RHI STATE to PASSIVE on all virtual servers, the Citrix ADC always advertises the route for the VIP address.
- If you set RHI STATE to ACTIVE on all virtual servers, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers is in UP state. *If you set RHI STATE to ACTIVE on some and PASSIVE on others, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers, whose RHI STATE set to ACTIVE, is in UP state.

Possible values: ONE_VSERVER, ALL_VSERVERS, NONE, VSVR_CNTRLD Default value: ONE_VSERVER

ospfLSAType Type of LSAs to be used by the OSPF protocol, running on the Citrix ADC, for advertising the route for this VIP address.

Possible values: TYPE1, TYPE5 Default value: TYPE5

ospfArea ID of the area in which the type1 link-state advertisements (LSAs) are to be advertised for this virtual IP (VIP) address by the OSPF protocol running on the Citrix ADC. When this parameter is not set, the VIP is advertised on all areas. Default value: -1 Minimum value: 0 Maximum value: 4294967294LU

tag Tag value for the network/host route associated with this IP. Default value: 0 Minimum value: 0

vrID A positive integer that uniquely identifies a VMAC address for binding to this VIP address. This binding is used to set up Citrix ADCs in an active-active configuration using VRRP. Minimum value: 1 Maximum value: 255

icmpResponse Respond to ICMP requests for a Virtual IP (VIP) address on the basis of the states of the virtual servers associated with that VIP. Available settings function as follows:

- NONE - The Citrix ADC responds to any ICMP request for the VIP address, irrespective of the states of the virtual servers associated with the address.
- ONE VSERVER - The Citrix ADC responds to any ICMP request for the VIP address if at least one of the associated virtual servers is in UP state.
- ALL VSERVER - The Citrix ADC responds to any ICMP request for the VIP address if all of the associated virtual servers are in UP state.
- VSVR_CNTRLD - The behavior depends on the ICMP VSERVER RESPONSE setting on all the associated virtual servers.

The following settings can be made for the ICMP VSERVER RESPONSE parameter on a virtual server:

- If you set ICMP VSERVER RESPONSE to PASSIVE on all virtual servers, Citrix ADC always responds.
- If you set ICMP VSERVER RESPONSE to ACTIVE on all virtual servers, Citrix ADC responds if even one virtual server is UP.
- When you set ICMP VSERVER RESPONSE to ACTIVE on some and PASSIVE on others, Citrix ADC responds if even one virtual server set to ACTIVE is UP.

Possible values: NONE, ONE_VSERVER, ALL_VSERVERS, VSVR_CNTRLD Default value: 5

arpResponse Respond to ARP requests for a Virtual IP (VIP) address on the basis of the states of the virtual servers associated with that VIP. Available settings function as follows:

- NONE - The Citrix ADC responds to any ARP request for the VIP address, irrespective of the states of the virtual servers associated with the address.
- ONE VSERVER - The Citrix ADC responds to any ARP request for the VIP address if at least one of the associated virtual servers is in UP state.
- ALL VSERVER - The Citrix ADC responds to any ARP request for the VIP address if all of the associated virtual servers are in UP state.

Possible values: NONE, ONE_VSERVER, ALL_VSERVERS Default value: 5

ownerDownResponse in cluster system, if the owner node is down, whether should it respond to icmp/arp

Possible values: YES, NO Default value: YES

arpOwner The arp owner in a Cluster for this IP address. It can vary from 0 to 31. Default value: 255 Minimum value: 0

mptcpAdvertise If enabled, this IP will be advertised by Citrix ADC to MPTCP enabled clients as part of ADD_ADDR option.

Possible values: YES, NO Default value: NO

Example

set ns ip 10.102.4.123 -arp ENABLED

ns-ip6

The following operations can be performed on "ns-ip6":

set| rm| add| show| unset|

set ns ip6

Modifies the specified parameters of an IPv6 address configured on the Citrix ADC.

Synopsis

set ns ip6 (<IPv6Address>@) [-ospf6LSAType (INTRA_AREA | EXTERNAL)]

Arguments

IPv6Address IPv6 address whose parameters you want to modify.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

nd The state of ND responses for the entity.

Possible values: ENABLED, DISABLED Default value: ENABLED

icmp The state of ICMP responses for the entity.

Possible values: ENABLED, DISABLED Default value: ENABLED

vServer The state of vserver attribute for this IP entity.

Possible values: ENABLED, DISABLED Default value: ENABLED

telnet The state of telnet access to this IP entity.

Possible values: ENABLED, DISABLED Default value: ENABLED

ftp The state of ftp access to this IP entity.

Possible values: ENABLED, DISABLED Default value: ENABLED

gui The state of GUI access to this IP entity.

Possible values: ENABLED, SECUREONLY, DISABLED Default value: ENABLED

ssh The state of SSH access to this IP entity.

Possible values: ENABLED, DISABLED Default value: ENABLED

snmp The state of SNMP access to this IP entity.

Possible values: ENABLED, DISABLED Default value: ENABLED

mgmtAccess The state of management access to this IP entity.

Possible values: ENABLED, DISABLED Default value: DISABLED

ownerDownResponse in cluster system, if the owner node is down, whether should it respond to icmp/arp

Possible values: YES, NO Default value: YES

restrictAccess Status of ports not used for management access (blocked/open) for the entity.

Possible values: ENABLED, DISABLED Default value: DISABLED

state Enable or disable the IP address.

Possible values: DISABLED, ENABLED Default value: ENABLED

map Mapped IPV4 address for the IPV6 address.

decrementHopLimit Decrement Hop Limit by 1 when ENABLED.This setting is applicable only for UDP traffic.

Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicRouting Allow dynamic routing on this IP address. Specific to Subnet IPv6 (SNIP6) address.

Possible values: ENABLED, DISABLED Default value: DISABLED

hostRoute Option to push the VIP6 to ZebOS routing table for Kernel route redistribution through dynamic routing protocols.

Possible values: ENABLED, DISABLED

advertiseOnDefaultPartition Advertise VIPs from Shared VLAN on Default Partition

Possible values: ENABLED, DISABLED Default value: DISABLED

networkRoute Option to push the SNIP6 subnet to ZebOS routing table for Kernel route redistribution through dynamic routing protocol.

Possible values: ENABLED, DISABLED

ip6hostRtGw IPv6 address of the gateway for the route. If Gateway is not set, VIP uses :: as the gateway. Default value: 0

metric Integer value to add to or subtract from the cost of the route advertised for the VIP6 address. Minimum value: -16777215

vserverRHILevel Advertise or do not advertise the route for the Virtual IP (VIP6) address on the basis of the state of the virtual servers associated with that VIP6.

- NONE - Advertise the route for the VIP6 address, irrespective of the state of the virtual servers associated with the address.
- ONE VSERVER - Advertise the route for the VIP6 address if at least one of the associated virtual servers is in UP state.
- ALL VSERVER - Advertise the route for the VIP6 address if all of the associated virtual servers are in UP state.
- VSVR_CNTRLD. Advertise the route for the VIP address according to the RHIstate (RHI STATE) parameter setting on all the associated virtual servers of the VIP address along with their states.

When Vserver RHI Level (RHI) parameter is set to VSVR_CNTRLD, the following are different RHI behaviors for the VIP address on the basis of RHIstate (RHI STATE) settings on the virtual servers associated with the VIP address:

- If you set RHI STATE to PASSIVE on all virtual servers, the Citrix ADC always advertises the route for the VIP address.
- If you set RHI STATE to ACTIVE on all virtual servers, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers is in UP state. *If you set RHI STATE to ACTIVE on some and PASSIVE on others, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers, whose RHI STATE set to ACTIVE, is in UP state.

Possible values: ONE_VSERVER, ALL_VSERVERS, NONE, VSVR_CNTRLD Default value: ONE_VSERVER

ospf6LSAType Type of LSAs to be used by the IPv6 OSPF protocol, running on the Citrix ADC, for advertising the route for the VIP6 address.

Possible values: INTRA_AREA, EXTERNAL Default value: EXTERNAL

ospfArea ID of the area in which the Intra-Area-Prefix LSAs are to be advertised for the VIP6 address by the IPv6 OSPF protocol running on the Citrix ADC. When ospfArea is not set, VIP6 is advertised on all areas. Default value: -1 Minimum value: 0 Maximum value: 4294967294LU

tag Tag value for the network/host route associated with this IP. Default value: 0 Minimum value: 0

vrID6 A positive integer that uniquely identifies a VMAC address for binding to this VIP address. This binding is used to set up Citrix ADCs in an active-active configuration using VRRP. Minimum value: 1 Maximum value: 255

ndOwner NdOwner in Cluster for VIPS and Striped SNIPS Default value: 255 Minimum value: 0

mptcpAdvertise If enabled, this IP will be advertised by Citrix ADC to MPTCP enabled clients as part of ADD_ADDR option.

Possible values: YES, NO Default value: NO

Example

set ns ip6 2001::a -map 10.102.33.27

rm ns ip6

Removes an IPv6 address configured on the Citrix ADC.

Synopsis

rm ns ip6 <IPv6Address>@

Arguments

IPv6Address IPv6 address that you want to remove.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

Example

rm ns ip6 2002::5

add ns ip6

Creates an IPv6 address on the Citrix ADC.

Synopsis

add ns ip6 <IPv6Address>@ [-type <type> [-hostRoute (ENABLED | DISABLED) [-ospf6LSAType (INTRA_AREA | EXTERNAL)]]]

Arguments

IPv6Address IPv6 address to create on the Citrix ADC.

scope Scope of the IPv6 address to be created. Cannot be changed after the IP address is created.

Possible values: global, link-local Default value: global

type Type of IP address to be created on the Citrix ADC. Cannot be changed after the IP address is created.

Possible values: NSIP, VIP, SNIP, GSLBsiteIP, ADNSsvcIP, RADIUSListenersvcIP, CLIP Default value: SNIP

vlan The VLAN number. Default value: 0 Minimum value: 0 Maximum value: 4094

nd Respond to Neighbor Discovery (ND) requests for this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

icmp Respond to ICMP requests for this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

vServer Enable or disable the state of all the virtual servers associated with this VIP6 address.

Possible values: ENABLED, DISABLED Default value: ENABLED

telnet Allow Telnet access to this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

ftp Allow File Transfer Protocol (FTP) access to this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

gui Allow graphical user interface (GUI) access to this IP address.

Possible values: ENABLED, SECUREONLY, DISABLED Default value: ENABLED

ssh Allow secure Shell (SSH) access to this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

snmp Allow Simple Network Management Protocol (SNMP) access to this IP address.

Possible values: ENABLED, DISABLED Default value: ENABLED

mgmtAccess Allow access to management applications on this IP address.

Possible values: ENABLED, DISABLED Default value: DISABLED

restrictAccess Block access to nonmanagement applications on this IP address. This option is applicable forMIP6s, SNIP6s, and NSIP6s, and is disabled by default. Nonmanagement applications can run on the underlying Citrix ADC Free BSD operating system.

Possible values: ENABLED, DISABLED Default value: DISABLED

dynamicRouting Allow dynamic routing on this IP address. Specific to Subnet IPv6 (SNIP6) address.

Possible values: ENABLED, DISABLED Default value: DISABLED

decrementHopLimit Decrement Hop Limit by 1 when ENABLED.This setting is applicable only for UDP traffic.

Possible values: ENABLED, DISABLED Default value: DISABLED

hostRoute Option to push the VIP6 to ZebOS routing table for Kernel route redistribution through dynamic routing protocols.

Possible values: ENABLED, DISABLED

advertiseOnDefaultPartition Advertise VIPs from Shared VLAN on Default Partition

Possible values: ENABLED, DISABLED Default value: DISABLED

networkRoute Option to push the SNIP6 subnet to ZebOS routing table for Kernel route redistribution through dynamic routing protocol.

Possible values: ENABLED, DISABLED

tag Tag value for the network/host route associated with this IP. Default value: 0 Minimum value: 0

ip6hostRtGw IPv6 address of the gateway for the route. If Gateway is not set, VIP uses :: as the gateway. Default value: 0

metric Integer value to add to or subtract from the cost of the route advertised for the VIP6 address. Minimum value: -16777215

vserverRHILevel Advertise or do not advertise the route for the Virtual IP (VIP6) address on the basis of the state of the virtual servers associated with that VIP6.

- NONE - Advertise the route for the VIP6 address, irrespective of the state of the virtual servers associated with the address.
- ONE VSERVER - Advertise the route for the VIP6 address if at least one of the associated virtual servers is in UP state.
- ALL VSERVER - Advertise the route for the VIP6 address if all of the associated virtual servers are in UP state.
- VSVR_CNTRLD. Advertise the route for the VIP address according to the RHIstate (RHI STATE) parameter setting on all the associated virtual servers of the VIP address along with their states.

When Vserver RHI Level (RHI) parameter is set to VSVR_CNTRLD, the following are different RHI behaviors for the VIP address on the basis of RHIstate (RHI STATE) settings on the virtual servers associated with the VIP address:

- If you set RHI STATE to PASSIVE on all virtual servers, the Citrix ADC always advertises the route for the VIP address.
- If you set RHI STATE to ACTIVE on all virtual servers, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers is in UP state. *If you set RHI STATE to ACTIVE on some and PASSIVE on others, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers, whose RHI STATE set to ACTIVE, is in UP state.

Possible values: ONE_VSERVER, ALL_VSERVERS, NONE, VSVR_CNTRLD Default value: ONE_VSERVER

ospf6LSAType Type of LSAs to be used by the IPv6 OSPF protocol, running on the Citrix ADC, for advertising the route for the VIP6 address.

Possible values: INTRA_AREA, EXTERNAL Default value: EXTERNAL

ospfArea ID of the area in which the Intra-Area-Prefix LSAs are to be advertised for the VIP6 address by the IPv6 OSPF protocol running on the Citrix ADC. When ospfArea is not set, VIP6 is advertised on all areas. Default value: -1 Minimum value: 0 Maximum value: 4294967294LU

state Enable or disable the IP address.

Possible values: DISABLED, ENABLED Default value: ENABLED

map Mapped IPV4 address for the IPV6 address.

vrID6 A positive integer that uniquely identifies a VMAC address for binding to this VIP address. This binding is used to set up Citrix ADCs in an active-active configuration using VRRP. Minimum value: 1 Maximum value: 255

ownerNode ID of the cluster node for which you are adding the IP address. Must be used if you want the IP address to be active only on the specific node. Can be configured only through the cluster IP address. Cannot be changed after the IP address is created. Default value: 255 Minimum value: 0

ownerDownResponse in cluster system, if the owner node is down, whether should it respond to icmp/arp

Possible values: YES, NO Default value: YES

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

ndOwner NdOwner in Cluster for VIPS and Striped SNIPS Default value: 255 Minimum value: 0

mptcpAdvertise If enabled, this IP will be advertised by Citrix ADC to MPTCP enabled clients as part of ADD_ADDR option.

Possible values: YES, NO Default value: NO

Example

add ns ip6 2001::a/96 -scope GLOBAL

show ns ip6

Displays settings of all the IPv6 addresses or of the specified IPv6 address configured on the Citrix ADC. To display settings of all the IPv6 addresses, run the command without any parameters. To display settings of a particular IPv6 address, specify the IPv6 address.

Synopsis

show ns ip6 [<IPv6Address>]

Arguments

IPv6Address IPv6 address whose settings you want the Citrix ADC to display.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

Output

scope Scope of the IPv6 address to be created. Cannot be changed after the IP address is created.

type The type of the IPV6 address

ipType The type of the IPv6 address

vlan The VLAN number.

nd Whether ND is enabled or disabled.

icmp Whether icmp is enabled or disabled.

vServer Whether vserver is enabled or disabled.

telnet Whether telnet is enabled or disabled.

ssh Whether ssh is enabled or disabled.

gui Whether gui is (enabled|SecureOnly|disabled).

snmp Whether snmp is enabled or disabled.

ftp Whether ftp is enabled or disabled.

mgmtAccess Whether management access is enabled or disabled.

restrictAccess Blocking of all ports not used for management access enabled or disabled

state The state of the IPV6 address

state Current state of this IP.

map Mapped IPV4 address for the IPV6 address.

decrementHopLimit Decrement Hop Limit by 1 when ENABLED.This setting is applicable only for UDP traffic.

dynamicRouting Allow dynamic routing on this IP address. Specific to Subnet IPv6 (SNIP6) address.

hostRoute Option to push the VIP6 to ZebOS routing table for Kernel route redistribution through dynamic routing protocols.

advertiseOnDefaultPartition Whether advertisment of VIPs of Shared VLAN is enabled or disabled.

networkRoute Option to push the SNIP6 subnet to ZebOS routing table for Kernel route redistribution through dynamic routing protocol.

tag Tag value for the network/host route associated with this IP.

ip6hostRtGw IPv6 address of the gateway for the route. If Gateway is not set, VIP uses :: as the gateway.

metric The metric value to be added or subtracted from the cost of the route advertised for this IPv6 entity.

vserverRHILevel Advertise or do not advertise the route for the Virtual IP (VIP6) address on the basis of the state of the virtual servers associated with that VIP6.

- NONE - Advertise the route for the VIP6 address, irrespective of the state of the virtual servers associated with the address.
- ONE VSERVER - Advertise the route for the VIP6 address if at least one of the associated virtual servers is in UP state.
- ALL VSERVER - Advertise the route for the VIP6 address if all of the associated virtual servers are in UP state.
- VSVR_CNTRLD. Advertise the route for the VIP address according to the RHIstate (RHI STATE) parameter setting on all the associated virtual servers of the VIP address along with their states.

When Vserver RHI Level (RHI) parameter is set to VSVR_CNTRLD, the following are different RHI behaviors for the VIP address on the basis of RHIstate (RHI STATE) settings on the virtual servers associated with the VIP address:

- If you set RHI STATE to PASSIVE on all virtual servers, the Citrix ADC always advertises the route for the VIP address.
- If you set RHI STATE to ACTIVE on all virtual servers, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers is in UP state. *If you set RHI

STATE to ACTIVE on some and PASSIVE on others, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers, whose RHI STATE set to ACTIVE, is in UP state.

VIPrtadv2BSD Whether this route is advertised to FreeBSD

VIPvserCount Number of vservers bound to this VIP

VIPvserDownCount Number of vservers bound to this VIP, which are down

ospf6LSAType The OSPF's route advertisement type.

ospfArea The area ID of the area in which OSPF INTRA AREA PREFIX LSAs should be advertised. When ospfArea is not set, LSAs are advertised in all areas.

ownerNode ID of the cluster node for which you are adding the IP address. Must be used if you want the IP address to be active only on the specific node. Can be configured only through the cluster IP address. Cannot be changed after the IP address is created.

stateflag vrID6 A positive integer that uniquely identifies a VMAC address for binding to this VIP address. This binding is used to set up Citrix ADCs in an active-active configuration using VRRP.

cfgflags This contains the flags for IP in DB

ipRefcount Used to keep reference count of IPv6

ownerDownResponse in cluster system, if the owner node is down, whether should it respond to icmp/arp

systemType The type of the System. Possible Values: Standalone, HA, Cluster. Used for display purpose.

ndOwner NdOwner in Cluster for VIPS and Striped SNIPS

operationalndOwner Operational ND6 Owner

mptcpAdvertise If enabled, this IP will be advertised by Citrix ADC to MPTCP enabled clients as part of ADD_ADDR option.

devno count

Example

show ns ip6

unset ns ip6

Modifies the parameters of an IPv6 address configured on the Citrix ADC..Refer to the set ns ip6 command for meanings of the arguments.

Synopsis

unset ns ip6 <IPv6Address>@

Example

unset ns ip6 2001::a -ospfArea

ns-job

The following operations can be performed on "ns-job":

show ns job

Displays the Job Details.

Synopsis

show ns job

Arguments

Id Running job id Minimum value: 0

Name Running job Name

Output

Id Running job id

Status Running job status

Progress Running job progress details

TimeElapsed Number of seconds since the job started.

ErrorCode Errcode for a particular job

Message Error message corresponding to the errorcode

devno count stateflag

Example

show ns job

ns-license

The following operations can be performed on "ns-license":

show ns license

Displays the state of all the licensed features.

Synopsis

show ns license

Arguments

Output

WL Web Logging.

SP Surge Protection.

LB Load Balancing.

CS Content Switching.

CR Cache Redirect.

CMP Compression.

DELTA Delta Compression.

SSL Secure Sockets Layer.

GSLB Global Server Load Balancing.

GSLBP GSLB Proximity.

Routing Routing.

CF Content Filter.

ContentAccelerator transparent Integrated Caching.

IC Integrated Caching.

SSLVPN SSL VPN.

AAA AAA

OSPF OSPF Routing.

RIP RIP Routing.

BGP BGP Routing.

REWRITE Rewrite.

IPv6PT IPv6 protocol translation

AppFw Application Firewall.

RESPONDER Responder.

AGEE NSXN ModelID Model Number ID. Represents different numbers for two types of licenses.:

- Bandwidth licenses - specifies the throughput bandwidth licensed for this appliance e.g. (For 20 Gbps) Model Number ID: 20000
- vCPU licenses - specifies number of vCPUs licensed for this appliance. e.g. (For 4 vCPU) Model Number ID: 4 vCPUs

push Citrix ADC Push.

AppFlow AppFlow.

CloudBridge CloudBridge.

CloudBridgeAppliance CloudExtenderAppliance ISIS ISIS Routing.

Cluster Clustering

CH Call Home.

AppQoE AppQoS

APPFLOWICA Appflow for ICA

isStandardLic Standard License

isEnterpriseLic Enterprise License

isPlatinumLic Platinum License

isSGwyLic Simple Gateway License

isSWGLic Secure Web Gateway License

DiskCaching Integrated Disk Cache

FEO Front End Optimization

LSN Large Scale NAT.

licensingMode Pooled Licensed.

CloudSubscriptionImage Cloud Subscription Image.

daysToExpiration Days to expire.

RDPProxy RDPPROXY.

Rep Reputation Services.

URLFiltering URL Filtering.

VideoOptimization Video Optimization.

ForwardProxy Forward Proxy.

SSLInterception SSL Interception.

RemoteContentInspection Remote Content Inspection.

AdaptiveTCP Adaptive TCP.

CQA Connection Quality Analytics.

Bot Bot Management.

APIGateway API Gateway

ns-licenseparameters

The following operations can be performed on "ns-licenseparameters":

unset| set| show|

unset ns licenseparameters

Use this command to remove ns licenseparameters settings.Refer to the set ns licenseparameters command for meanings of the arguments.

Synopsis

unset ns licenseparameters

set ns licenseparameters

Modifies the specified license parameters.

Synopsis

set ns licenseparameters

Arguments

alert1gracetimeout If ADC remains in grace for the configured hours then first grace alert will be raised Default value: 6 Minimum value: 0 Maximum value: 24

alert2gracetimeout If ADC remains in grace for the configured hours then major grace alert will be raised Default value: 240 Minimum value: 24 Maximum value: 720

licenseexpiryalerttime If ADC termed license is nearer to expiry then SNMP expiry alert will be raised Default value: 30 Minimum value: 1 Maximum value: 365

heartbeatinterval Heartbeat between ADC and Licenseserver is configurable and applicable in case of pooled licensing Default value: 280 Minimum value: 30 Maximum value: 280

inventoryrefreshinterval Inventory refresh interval between ADC and Licenseserver is configurable and applicable in case of pooled licensing Default value: 360 Minimum value: 45 Maximum value: 1440

show ns licenseparameters

Displays information about the license parameters.

Synopsis

show ns licenseparameters

Arguments

Output

alert1gracetimeout If ADC remains in grace for the configured hours then first grace alert will be raised

alert2gracetimeout If ADC remains in grace for the configured hours then major grace alert will be raised

licenseexpiryalerttime If ADC termed license is nearer to expiry then SNMP expiry alert will be raised

heartbeatinterval Heartbeat between ADC and Licenseserver is configurable and applicable in case of pooled licensing

inventoryrefreshinterval Inventory refresh interval between ADC and Licenseserver is configurable and applicable in case of pooled licensing

ns-licenseproxyserver

The following operations can be performed on "ns-licenseproxyserver":

set| add| rm| show|

set ns licenseproxyserver

Modifies the port of License proxy server.

Synopsis

set ns licenseproxyserver (<serverIP> | <serverName>) -port <positive_integer>

Arguments

serverIP IP address of the License proxy server to be modified.

serverName Name of the License proxy server to be modified.

port License proxy server port. Minimum value: 0

add ns licenseproxyserver

Adds License proxy server config to the appliance.

Synopsis

add ns licenseproxyserver (<serverIP> | <serverName>) -port <positive_integer>

Arguments

serverIP IP address of the License proxy server.

serverName Fully qualified domain name of the License proxy server.

port License proxy server port. Minimum value: 0

rm ns licenseproxyserver

Removes the License proxy server. You can specify the server by IP address or by name.

Synopsis

rm ns licenseproxyserver (<serverIP> | <serverName>)

Arguments

serverIP IP address of the License proxy server to be removed.

serverName Name of the License proxy server to be removed.

show ns licenseproxyserver

Displays information about an License proxy server. You can specify the server by IP address or by name.

Synopsis

show ns licenseproxyserver

Arguments

serverIP IP address of the License proxy server about which to display information.

serverName Name of the License proxy server about which to display information.

Output

port License proxy server port.

devno count stateflag

ns-licenseserver

The following operations can be performed on "ns-licenseserver":

set| show| add| rm|

set ns licenseserver

Modifies the port of License server.

Synopsis

set ns licenseserver (<licenseServerIP> | <serverName>)

Arguments

licenseServerIP IP address of the NTP server to be modified.

serverName Name of the NTP server to be modified.

port License server port. Default value: NS_LICENSE_DEFAULT_PORT Minimum value: 0

licensemode This paramter indicates type of license customer interested while configuring add/set licenseserver

Possible values: Pooled, VCPU, CICO, SelfManagedPool, SelfManagedvCPU

show ns licenseserver

Displays information about an License server. You can specify the server by IP address or by name.

Synopsis

show ns licenseserver

Arguments

licenseServerIP IP address of the NTP server about which to display information.

serverName Name of the NTP server about which to display information.

Output

port License server port.

status Status of license server.

grace Grace status of server.

gptimeleft Grace time left

type License Server type CLA/ADM.

devno count stateflag

add ns licenseserver

Adds License server config to the appliance.

Synopsis

add ns licenseserver (<licenseServerIP> | <serverName>)

Arguments

licenseServerIP IP address of the License server.

serverName Fully qualified domain name of the License server.

port License server port. Default value: NS_LICENSE_DEFAULT_PORT Minimum value: 0

forceUpdateIP If this flag is used while adding the licenseserver, existing config will be overwritten. Use this flag only if you are sure that the new licenseserver has the required capacity.

licensemode This paramter indicates type of license customer interested while configuring add/set licenseserver

Possible values: Pooled, VCPU, CICO, SelfManagedPool, SelfManagedvCPU

rm ns licenseserver

Removes the License server. You can specify the server by IP address or by name.

Synopsis

rm ns licenseserver (<licenseServerIP> | <serverName>)

Arguments

licenseServerIP IP address of the License server to be removed.

serverName Name of the License server to be removed.

ns-licenseserverpool

The following operations can be performed on "ns-licenseserverpool":

show ns licenseserverpool

Displays details of the appliance pooled license inventory.

Synopsis

show ns licenseserverpool

Arguments

getallLicenses If this flag is used while doing getinventory, it displays all licenses from licenseserver.

Output

InstanceTotal Instance Total.

InstanceAvailable Instance Available.

StandardBandwidthTotal Standard Bandwidth Total.

StandardBandwidthAvailable Standard Bandwidth Available.

EnterpriseBandwidthTotal Enterprise Bandwidth Total.

EnterpriseBandwidthAvailable Enterprise Bandwidth Available.

PlatinumBandwidthTotal Platinum Bandwidth Total.

PlatinumBandwidthAvailable Platinum Bandwidth Available.

StandardCPUTotal Standard CPU Total.

StandardCPUAvailable Standard CPU Available.

EnterpriseCPUTotal Enterprise CPU Total.

EnterpriseCPUAvailable Enterprise CPU Available.

PlatinumCPUTotal Platinum CPU Total.

PlatinumCPUAvailable Platinum CPU Available.

CPXInstanceTotal CP1000 Instance Total.

CPXInstanceAvailable CP1000 Instance Available.

VPX1STotal VPX1S Total.

VPX1SAvailable VPX1S Available.

VPX1PTotal VPX1P Total.

VPX1PAvailable VPX1P Available.

VPX5STotal VPX5S Total.

VPX5SAvailable VPX5S Available.

VPX5PTotal VPX5P Total.

VPX5PAvailable VPX5P Available.

VPX10STotal VPX10S Total.

VPX10SAvailable VPX10S Available.

VPX10ETotal VPX10E Total.

VPX10EAvailable VPX10E Available.

VPX10PTotal VPX10P Total.

VPX10PAvailable VPX10P Available.

VPX25STotal VPX25S Total.

VPX25SAvailable VPX25S Available.

VPX25ETotal VPX25E Total.

VPX25EAvailable VPX25E Available.

VPX25PTotal VPX25P Total.

VPX25PAvailable VPX25P Available.

VPX50STotal VPX50S Total.

VPX50SAvailable VPX50S Available.

VPX50ETotal VPX50E Total.

VPX50EAvailable VPX50E Available.

VPX50PTotal VPX50P Total.

VPX50PAvailable VPX50P Available.

VPX100STotal VPX100S Total.

VPX100SAvailable VPX100S Available.

VPX100ETotal VPX100E Total.

VPX100EAvailable VPX100E Available.

VPX100PTotal VPX100P Total.

VPX100PAvailable VPX100P Available.

VPX200STotal VPX200S Total.

VPX200SAvailable VPX200S Available.

VPX200ETotal VPX200E Total.

VPX200EAvailable VPX200E Available.

VPX200PTotal VPX200P Total.

VPX200PAvailable VPX200P Available.

VPX500STotal VPX500S Total.

VPX500SAvailable VPX500S Available.

VPX500ETotal VPX500E Total.

VPX500EAvailable VPX500E Available.

VPX500PTotal VPX500P Total.

VPX500PAvailable VPX500P Available.

VPX1000STotal VPX1000S Total.

VPX1000SAvailable VPX1000S Available.

VPX1000ETotal VPX1000E Total.

VPX1000EAvailable VPX1000E Available.

VPX1000PTotal VPX1000P Total.

VPX1000PAvailable VPX1000P Available.

VPX2000PTotal VPX2000P Total.

VPX2000PAvailable VPX2000P Available.

VPX3000STotal VPX3000S Total.

VPX3000SAvailable VPX3000S Available.

VPX3000ETotal VPX3000E Total.

VPX3000EAvailable VPX3000E Available.

VPX3000PTotal VPX3000P Total.

VPX3000PAvailable VPX3000P Available.

VPX4000PTotal VPX4000P Total.

VPX4000PAvailable VPX4000P Available.

VPX5000STotal VPX5000S Total.

VPX5000SAvailable VPX5000S Available.

VPX5000ETotal VPX5000E Total.

VPX5000EAvailable VPX5000E Available.

VPX5000PTotal VPX5000P Total.

VPX5000PAvailable VPX5000P Available.

VPX8000STotal VPX8000S Total.

VPX8000SAvailable VPX8000S Available.

VPX8000ETotal VPX8000E Total.

VPX8000EAvailable VPX8000E Available.

VPX8000PTotal VPX8000P Total.

VPX8000PAvailable VPX8000P Available.

VPX10000STotal VPX10000S Total.

VPX10000SAvailable VPX10000S Available.

VPX10000ETotal VPX10000E Total.

VPX10000EAvailable VPX10000E Available.

VPX10000PTotal VPX10000P Total.

VPX10000PAvailable VPX10000P Available.

VPX15000STotal VPX15000S Total.

VPX15000SAvailable VPX15000S Available.

VPX15000ETotal VPX15000E Total.

VPX15000EAvailable VPX15000E Available.

VPX15000PTotal VPX15000P Total.

VPX15000PAvailable VPX15000P Available.

VPX25000STotal VPX25000S Total.

VPX25000SAvailable VPX25000S Available.

VPX25000ETotal VPX25000E Total.

VPX25000EAvailable VPX25000E Available.

VPX25000PTotal VPX25000P Total.

VPX25000PAvailable VPX25000P Available.

VPX40000STotal VPX40000S Total.

VPX40000SAvailable VPX40000S Available.

VPX40000ETotal VPX40000E Total.

VPX40000EAvailable VPX40000E Available.

VPX40000PTotal VPX40000P Total.

VPX40000PAvailable VPX40000P Available.

VPX100000STotal VPX100000S Total.

VPX100000SAvailable VPX100000S Available.

VPX100000ETotal VPX100000E Total.

VPX100000EAvailable VPX100000E Available.

VPX100000PTotal VPX100000P Total.

VPX100000PAvailable VPX100000P Available.

licensemode This paramter indicates type of license customer interested while configuring add/set licenseserver

ns-limitIdentifier

The following operations can be performed on "ns-limitIdentifier":

show| unset| stat| add| set| rm|

show ns limitIdentifier

Displays information about a rate limit identifier.

Synopsis

show ns limitIdentifier

Arguments

limitIdentifier Name of the rate limit identifier about which to display information. If a name is not provided, information about all rate limit identifiers is shown.

Output

ngname Nodegroup name to which this identifier belongs to.

threshold Maximum number of requests that are allowed in the given timeslice when requests (mode is set as REQUEST_RATE) are tracked per timeslice. When connections (mode is set as CONNECTION) are tracked, it is the total number of connections that would be let through.

timeSlice Defines the time interval in msecs specified in multiples of 10 msec during which the requests are tracked to see if they cross the threshold. It is used and displayed only when the mode is REQUEST_RATE while tracking request rate and for defining the trap timeslice.

mode Defines the type of traffic to be tracked.

- REQUEST_RATE - Tracks requests/timeslice.
- CONNECTION - Tracks active transactions.

Examples

1. To permit 20 requests in 10 ms and 2 traps in 10 ms: add limitidentifier limit_req -mode request_rate -limitType smooth -timeslice 1000 -Threshold 2000 -trapsInTimeSlice 200
2. To permit 50 requests in 10 ms: set limitidentifier limit_req -mode request_rate -timeslice 1000 -Threshold 5000 -limitType smooth
3. To permit 1 request in 40 ms: set limitidentifier limit_req -mode request_rate -timeslice 2000 -Threshold 50 -limitType smooth
4. To permit 1 request in 200 ms and 1 trap in 130 ms: set limitidentifier limit_req -mode request_rate -timeslice 1000 -Threshold 5 -limitType smooth -trapsInTimeSlice 8
5. To permit 5000 requests in 1000 ms and 200 traps in 1000 ms: set limitidentifier limit_req -mode request_rate -timeslice 1000 -Threshold 5000 -limitType BURSTY

limitType Smooth or bursty request type.

- SMOOTH - When you want the permitted number of requests in a given interval of time to be spread evenly across the timeslice
- BURSTY - When you want the permitted number of requests to exhaust the quota anytime within the timeslice. This argument is needed only when the mode is set to REQUEST_RATE.

selectorName Name of the rate limit selector. If this argument is NULL, rate limiting will be applied on all traffic received by the virtual server or the Citrix ADC (depending on whether the limit identifier is bound to a virtual server or globally) without any filtering.

stateflag This is used internally to identify ip addresses returned.

hits The number of times this identifier was evaluated.

drop The number of times action was taken.

rule Rule.

time Time interval considered for rate limiting

total Maximum number of requests permitted in the computed timeslice

maxBandwidth The maximum bandwidth in kbps permitted

trapsInTimeSlice The maximum bandwidth permitted in kbps

trapsComputedInTimeSlice The number of traps that would be sent in the timeslice configured.

computedTrapTimeSlice The time interval computed for sending traps.

referenceCount Total number of transactions pointing to this entry.

devno count

Example

show ns limitIdentifier limit_id

unset ns limitIdentifier

Use this command to remove ns limitIdentifier settings.Refer to the set ns limitIdentifier command for meanings of the arguments.

Synopsis

unset ns limitIdentifier <limitIdentifier>

stat ns limitIdentifier

Display statistics of a identifier.

Synopsis

stat ns limitIdentifier [<name>] [-sortBy Hits]

Arguments

name The name of the identifier.

pattern Pattern for the selector field, ? means field is required, * means field value does not matter, anything else is a regular pattern

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

sortBy use this argument to sort by specific key

Possible values: Hits

sortOrder use this argument to specify sort order

Possible values: ascending, descending Default value: SORT_DESCENDING

Output

count devno stateflag

Counters

Rate Limit Identifier Hits (Hits) Total hits.

Rate Limit Identifier Drops (Drops) Total drops

Rate Limit Session Hits (Hits) Total hits.

Related Commands

- stat ns partition

add ns limitIdentifier

Adds a limit identifier to check if the amount of traffic exceeds a specified value, within a particular time interval.

Synopsis

add ns limitIdentifier <limitIdentifier> [-mode <mode>]

Arguments

limitIdentifier Name for a rate limit identifier. Must begin with an ASCII letter or underscore (_) character, and must consist only of ASCII alphanumeric or underscore characters. Reserved words must not be used.

threshold Maximum number of requests that are allowed in the given timeslice when requests (mode is set as REQUEST_RATE) are tracked per timeslice. When connections (mode is set as

CONNECTION) are tracked, it is the total number of connections that would be let through. Default value: 1 Minimum value: 1

timeSlice Time interval, in milliseconds, specified in multiples of 10, during which requests are tracked to check if they cross the threshold. This argument is needed only when the mode is set to REQUEST_RATE. Default value: 1000 Minimum value: 10

mode Defines the type of traffic to be tracked.

- REQUEST_RATE - Tracks requests/timeslice.
- CONNECTION - Tracks active transactions.

Examples

1. To permit 20 requests in 10 ms and 2 traps in 10 ms: add limitidentifier limit_req -mode request_rate -limitType smooth -timeslice 1000 -Threshold 2000 -trapsInTimeSlice 200
2. To permit 50 requests in 10 ms: set limitidentifier limit_req -mode request_rate -timeslice 1000 -Threshold 5000 -limitType smooth
3. To permit 1 request in 40 ms: set limitidentifier limit_req -mode request_rate -timeslice 2000 -Threshold 50 -limitType smooth
4. To permit 1 request in 200 ms and 1 trap in 130 ms: set limitidentifier limit_req -mode request_rate -timeslice 1000 -Threshold 5 -limitType smooth -trapsInTimeSlice 8
5. To permit 5000 requests in 1000 ms and 200 traps in 1000 ms: set limitidentifier limit_req -mode request_rate -timeslice 1000 -Threshold 5000 -limitType BURSTY

Possible values: CONNECTION, REQUEST_RATE, NONE Default value: REQUEST_RATE

limitType Smooth or bursty request type.

- SMOOTH - When you want the permitted number of requests in a given interval of time to be spread evenly across the timeslice
- BURSTY - When you want the permitted number of requests to exhaust the quota anytime within the timeslice. This argument is needed only when the mode is set to REQUEST_RATE.

Possible values: BURSTY, SMOOTH Default value: BURSTY

selectorName Name of the rate limit selector. If this argument is NULL, rate limiting will be applied on all traffic received by the virtual server or the Citrix ADC (depending on whether the limit identifier is bound to a virtual server or globally) without any filtering.

maxBandwidth Maximum bandwidth permitted, in kbps. Minimum value: 0 Maximum value: 4294967287

trapsInTimeSlice Number of traps to be sent in the timeslice configured. A value of 0 indicates that traps are disabled. Minimum value: 0 Maximum value: 65535

Example

add ns limitIdentifier limit_id -threshold 2 -timeSlice 5000 -mode CONNECTION -selectorName sel_1 -maxBandwidth 24 -trapsInTimeSlice 8

set ns limitIdentifier

Modifies the attributes of a rate limit identifier.

Synopsis

set ns limitIdentifier <limitIdentifier> [-mode <mode>]

Arguments

limitIdentifier Name of the rate limit identifier to be modified.

threshold Maximum number of requests that are allowed in the given timeslice when requests (mode is set as REQUEST_RATE) are tracked per timeslice. When connections (mode is set as CONNECTION) are tracked, it is the total number of connections that would be let through. Default value: 1 Minimum value: 1

timeSlice Time interval, in milliseconds, specified in multiples of 10, during which requests are tracked to check if they cross the threshold. This argument is needed only when the mode is set to REQUEST_RATE. Default value: 1000 Minimum value: 10

mode Defines the type of traffic to be tracked.

- REQUEST_RATE - Tracks requests/timeslice.
- CONNECTION - Tracks active transactions.

Examples

1. To permit 20 requests in 10 ms and 2 traps in 10 ms: add limitidentifier limit_req -mode request_rate -limitType smooth -timeslice 1000 -Threshold 2000 -trapsInTimeSlice 200
2. To permit 50 requests in 10 ms: set limitidentifier limit_req -mode request_rate -timeslice 1000 -Threshold 5000 -limitType smooth

3. To permit 1 request in 40 ms: set limitidentifier limit_req -mode request_rate -timeslice 2000 -Threshold 50 -limitType smooth
4. To permit 1 request in 200 ms and 1 trap in 130 ms: set limitidentifier limit_req -mode request_rate -timeslice 1000 -Threshold 5 -limitType smooth -trapsInTimeSlice 8
5. To permit 5000 requests in 1000 ms and 200 traps in 1000 ms: set limitidentifier limit_req -mode request_rate -timeslice 1000 -Threshold 5000 -limitType BURSTY

Possible values: CONNECTION, REQUEST_RATE, NONE Default value: REQUEST_RATE

limitType Smooth or bursty request type.

- SMOOTH - When you want the permitted number of requests in a given interval of time to be spread evenly across the timeslice
- BURSTY - When you want the permitted number of requests to exhaust the quota anytime within the timeslice. This argument is needed only when the mode is set to REQUEST_RATE.

Possible values: BURSTY, SMOOTH Default value: BURSTY

selectorName Name of the rate limit selector. If this argument is NULL, rate limiting will be applied on all traffic received by the virtual server or the Citrix ADC (depending on whether the limit identifier is bound to a virtual server or globally) without any filtering.

maxBandwidth Maximum bandwidth permitted, in kbps. Minimum value: 0 Maximum value: 4294967287

trapsInTimeSlice Number of traps to be sent in the timeslice configured. A value of 0 indicates that traps are disabled. Minimum value: 0 Maximum value: 65535

Example

set ns limitIdentifier limit_id -threshold 2 -timeSlice 5000 -mode CONNECTION -selectorName sel_1 -maxBandwidth 24 -trapsInTimeSlice 8

rm ns limitIdentifier

Removes a rate limit identifier from the appliance.

Synopsis

rm ns limitIdentifier <limitIdentifier>

Arguments

limitIdentifier Name of the rate limit identifier to be removed.

Example

rm ns limitIdentifier limit_id

ns-limitSelector

The following operations can be performed on "ns-limitSelector":

rm| show| add| set| unset|

rm ns limitSelector

NOTE: This command is deprecated.Replaced by "stream selector"

Synopsis

Arguments

selectorName

show ns limitSelector

NOTE: This command is deprecated.Replaced by "stream selector"

Synopsis

Arguments

selectorName

Output

rule stateflag devno count

add ns limitSelector

NOTE: This command is deprecated.Replaced by "stream selector"

Synopsis

Arguments

selectorName rule

set ns limitSelector

NOTE: This command is deprecated.

Synopsis

Arguments

selectorName rule

unset ns limitSelector

Use this command to remove ns limitSelector settings.Refer to the set ns limitSelector command for meanings of the arguments.NOTE: This command is deprecated.

Synopsis

ns-limitSessions

The following operations can be performed on "ns-limitSessions":

show| clear|

show ns limitSessions

Displays the rate limit sessions available on the appliance.

Synopsis

show ns limitSessions <limitIdentifier>

Arguments

limitIdentifier Name of the rate limit identifier for which to display the sessions.

detail Show the individual hash values.

Output

timeout The time remaining on the session before a flush can be attempted. If active transactions are present the session will not be flushed

hits The number of times this entry was hit.

drop The number of times action was taken.

number The hash of the matched selectlets.

name The string formed by gathering selectlet values.

unit Total computed hash of the matched selectlets.

flags Used internally to identify ip addresses.

referenceCount Total number of transactions pointing to this entry. Its the sum total of the connection and bandwidth references

maxBandwidth The current bandwidth

SelectorIPV61 First IPV6 address gathered.

SelectorIPV62 Second IPV6 address gathered.

flag Used internally to identify ipv6 addresses.

devno count stateflag

clear ns limitSessions

Clears the rate limit sessions available on the appliance.

Synopsis

clear ns limitSessions <limitIdentifier>

Arguments

limitIdentifier Name of the rate limit identifier for which the sessions must be cleared.

ns-memory

The following operations can be performed on "ns-memory":

stat ns memory

Displays memory statistics of Citrix ADC features.

Synopsis

stat ns memory

Arguments

pool Feature name for which to display memory statistics.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Maximum Allocation Failed (MB) (MemTotAllocFailed) Total system memory allocation failed.

Maximum Allocation Failed (MB) (MemTotAllocFailed) Total system memory allocation failed.

Allocation failure (AllocF) Memory allocation failure for particular feature.

Percentage of memory allocated (Alloc(%)) Percentage of Citrix ADC memory used by the feature.

Total memory Allocated (KB) (CurAlloc(KB)) Total current Citrix ADC memory available for use by the feature, in kilobytes.

Maximum Allocation Failed (MB) (MemTotAllocFailed) Total system memory allocation failed.

Related Commands

- stat ns partition

ns-memrecovery

The following operations can be performed on "ns-memrecovery":

start ns memrecovery

Start memory recovery.

Synopsis

start ns memrecovery

Arguments

percentage Percentage of memory to be recovered from freepools Default value: 10 Minimum value: 5 Maximum value: 90

Example

start nsmemrecovery -percentage 30

ns-migration

The following operations can be performed on "ns-migration":

start| show| stop|

start ns migration

Start the Migration Operation which will start the migration of sessions

Synopsis

start ns migration

Example

start ns migration

show ns migration

Show the status of ISSU migration for the current node

Synopsis

show ns migration

Arguments

dumpsession Displays the current active migrated session details, if DUMPSESSION option is YES.

Possible values: YES, NO Default value: NO

Output

migrationStatus ISSU Migration Status

migrationStartTime Timestamp for start migration

migrationEndTime Timestamp for migration complete

migrationRollbackStartTime Timestamp for start migration rollback

dumpsession srcIP IP address to match against the source IP address of an incoming IPv4 packet.

srcPort Port number to match against the source port number of an incoming IPv4 packet.

destIP IP address to match against the destination IP address of an incoming IPv4 packet.

destPort Port number to match against the destination port number of an incoming IPv4 packet.

timeout Time for which the connection is idle.

migdfdsessionsallocated Number of migration sessions allocated.

migdfdsessionsactive Number of migration sessions active.

migl4sessionsallocated Number of migration sessions allocated.

migl4sessionsactive Number of migration sessions active.

migdfdsessionsallocatedrollback Number of migration sessions allocated.

migdfdsessionsactiverollback Number of migration sessions active.

migl4sessionsallocatedrollback Number of migration sessions allocated.

migl4sessionsactiverollback Number of migration sessions active.

mighastateflag Current master state in HA.

devno count stateflag

Example

show ns migration

stop ns migration

Stop the running Migration operation

Synopsis

stop ns migration

Example

stop ns migration

ns-mode

The following operations can be performed on "ns-mode":

show| disable| enable|

show ns mode

Displays the current state of Citrix ADC modes.

Synopsis

show ns mode

Arguments

Output

Mode Mode to be enabled. Multiple modes can be specified by providing a blank space between each mode.

FR Fast Ramp.

L2 Layer 2 mode.

USIP Use Source IP.

CKA Client Keep-alive.

TCPB TCP Buffering.

MBF MAC-based forwarding.

Edge Edge configuration.

USNIP Use Subnet IP.

L3 Layer 3 mode (ip forwarding).

PMTUD Path MTU Discovery.

Mediaclassification mediaclassification

SRADV Static Route Advertisement.

DRADV Direct Route Advertisement.

IRADV Intranet Route Advertisement.

SRADV6 Ipv6 Static Route Advertisement.

DRADV6 Ipv6 Direct Route Advertisement.

BridgeBPDUs BPDU Bridging Mode.

ULFD Unified Logging Framework Mode for adding/removing ULF services

disable ns mode

Disables Citrix ADC mode(s).

Synopsis

disable ns mode <Mode> ...

Arguments

Mode Mode to be disabled. Multiple modes can be specified by providing a blank space between each mode.

Example

This example shows the command to disable the system's client keep-alive feature: disable ns mode CKA

enable ns mode

Enables Citrix ADC mode(s).

Synopsis

enable ns mode <Mode> ...

Arguments

Mode Mode to be enabled. Multiple modes can be specified by providing a blank space between each mode.

Example

This CLI command enables the system's client keep-alive feature: enable ns mode CKA

ns-nsconf

The following operations can be performed on "ns-ns.conf":

show ns nsconf

Displays the saved configurations.

Synopsis

show ns ns.conf

Arguments

Output

textBlob Text of the last saved configuration.

Related Commands

- save config, show runningconfig

ns-param

The following operations can be performed on "ns-param":

show| unset| set|

show ns param

Displays the information of the parameters of the Citrix ADC that were set by using the 'set ns param' command.

Synopsis

show ns param

Arguments

Output

httpPort The HTTP ports on the Web server.

maxConn Maximum Number of Connections.

maxReq Maxmimum Number of requests that can be handled.

cip Insertion of client IP address into the HTTP header.

cipHeader The text that will be used as the client IP header.

cookieversion Version of the cookie inserted by the system.

secureCookie Enable or disable secure flag for persistence cookie.

pmtuMin Minimum path MTU value that Citrix ADC will process in the ICMP fragmentation needed message. If the ICMP message contains a value less than this value, then this value is used instead.

pmtuTimeout Interval, in minutes, for flushing the PMTU entries.

ftpPortRange Minimum and maximum port (port range) that FTP services are allowed to use.

crPortRange Port range for cache redirection services.

timezone Time zone for the Citrix ADC. Name of the time zone should be specified as argument.

grantQuotaMaxClient Percentage of shared quota to be granted at a time for maxClient.

exclusiveQuotaMaxClient Percentage of maxClient to be given to PEs.

grantQuotaSpillOver Percentage of shared quota to be granted at a time for spillover.

exclusiveQuotaSpillOver Percentage of maximum limit to be given to PEs.

useproxyport Enable/Disable use_proxy_port setting

internaluserlogin Enables/disables the internal user from logging in to the appliance. Before disabling internal user login, you must have key-based authentication set up on the appliance. The file name for the key pair must be "ns_comm_key".

aftpAllowRandomSourcePort Allow the FTP server to come from a random source port for active FTP data connections

icaPorts The ICA ports on the Web server. This allows the system to perform connection off-load for any client request that has a destination port matching one of these configured ports.

tcpCIP Enable or disable the insertion of the client TCP/IP header in TCP payload passed from the client to one, some, or all servers attached to the system. The passed address can then be accessed through a minor modification to the server.

servicePathIngressVLAN VLAN on which the subscriber traffic arrives on the appliance.

secureicaPorts The Secure ICA ports on the Web server. This allows the system to perform connection off-load for any client request that has a destination port matching one of these configured ports.

mgmthttpport This allow the configuration of management HTTP port.

mgmthttpsport This allows the configuration of management HTTPS port.

proxyProtocol Disable/Enable v1 or v2 proxy protocol header for client info insertion

advancedAnalyticsStats Advnced analytics stats collection.

autoscaleOption 64 bits are provided for communication between ADM and ADC in cloud deployments. Currently LSB 3 bits are used.0x01=>AWS,0x02=>Azure,0x04=>GCP

ipTtl Set the IP Time to Live (TTL) and Hop Limit value for all outgoing packets from Citrix ADC.

unset ns param

Removes the attributes of the Citrix ADC parameters. Attributes for which a default value is available revert to their default values. Refer to the 'set ns param' command for a description of the parameters..Refer to the set ns param command for meanings of the arguments.

Synopsis

unset ns param

set ns param

Sets the parameters of the Citrix ADC.

Synopsis

set ns param [-ftpPortRange <int>] [-crPortRange <int>]

Arguments

httpPort HTTP ports on the web server. This allows the system to perform connection off-load for any client request that has a destination port matching one of these configured ports. Minimum value: 1 Maximum value: 65535

maxConn Maximum number of connections that will be made from the appliance to the web server(s) attached to it. The value entered here is applied globally to all attached servers. Default value: 0 Minimum value: 0 Maximum value: 4294967294

maxReq Maximum number of requests that the system can pass on a particular connection between the appliance and a server attached to it. Setting this value to 0 allows an unlimited number of requests to be passed. This value is overridden by the maximum number of requests configured on the individual service. Minimum value: 0 Maximum value: 65535

cip Enable or disable the insertion of the actual client IP address into the HTTP header request passed from the client to one, some, or all servers attached to the system. The passed address can then be accessed through a minor modification to the server.

- If the CIP header is specified, it will be used as the client IP header.
- If the CIP header is not specified, the value that has been set will be used as the client IP header.

Possible values: ENABLED, DISABLED

cipHeader Text that will be used as the client IP address header.

cookieversion Version of the cookie inserted by the system.

Possible values: 0, 1

secureCookie Enable or disable secure flag for persistence cookie.

Possible values: ENABLED, DISABLED Default value: ENABLED

pmtuMin Minimum path MTU value that Citrix ADC will process in the ICMP fragmentation needed message. If the ICMP message contains a value less than this value, then this value is used instead. Default value: 576 Minimum value: 168 Maximum value: 1500

pmtuTimeout Interval, in minutes, for flushing the PMTU entries. Default value: 10 Minimum value: 1 Maximum value: 1440

ftpPortRange Minimum and maximum port (port range) that FTP services are allowed to use. Minimum value: 1024 Maximum value: 64000

crPortRange Port range for cache redirection services. Minimum value: 1 Maximum value: 65535

timezone Time zone for the Citrix ADC. Name of the time zone should be specified as argument. Default value: CoordinatedUniversalTime

grantQuotaMaxClient Percentage of shared quota to be granted at a time for maxClient. Default value: 10 Minimum value: 0 Maximum value: 100

exclusiveQuotaMaxClient Percentage of maxClient to be given to PEs. Default value: 80 Minimum value: 0 Maximum value: 100

grantQuotaSpillOver Percentage of shared quota to be granted at a time for spillover. Default value: 10 Minimum value: 0 Maximum value: 100

exclusiveQuotaSpillOver Percentage of maximum limit to be given to PEs. Default value: 80 Minimum value: 0 Maximum value: 100

useproxyport Enable/Disable use_proxy_port setting

Possible values: ENABLED, DISABLED Default value: ENABLED

internaluserlogin Enables/disables the internal user from logging in to the appliance. Before disabling internal user login, you must have key-based authentication set up on the appliance. The file name for the key pair must be "ns_comm_key".

Possible values: ENABLED, DISABLED Default value: ENABLED

aftpAllowRandomSourcePort Allow the FTP server to come from a random source port for active FTP data connections

Possible values: ENABLED, DISABLED Default value: DISABLED

icaPorts The ICA ports on the Web server. This allows the system to perform connection off-load for any client request that has a destination port matching one of these configured ports. Minimum value: 1

tcpCIP Enable or disable the insertion of the client TCP/IP header in TCP payload passed from the client to one, some, or all servers attached to the system. The passed address can then be accessed through a minor modification to the server.

Possible values: ENABLED, DISABLED Default value: DISABLED

servicePathIngressVLAN VLAN on which the subscriber traffic arrives on the appliance. Minimum value: 1

secureicaPorts The Secure ICA ports on the Web server. This allows the system to perform connection off-load for any client request that has a destination port matching one of these configured ports. Minimum value: 1

mgmthttpport This allow the configuration of management HTTP port. Default value: 80 Minimum value: 1 Maximum value: 65534

mgmthttpsport This allows the configuration of management HTTPS port. Default value: 443 Minimum value: 1 Maximum value: 65534

proxyProtocol Disable/Enable v1 or v2 proxy protocol header for client info insertion

Possible values: ENABLED, DISABLED Default value: DISABLED

advancedAnalyticsStats Disable/Enable advanace analytics stats

Possible values: ENABLED, DISABLED Default value: DISABLED

ipTtl Set the IP Time to Live (TTL) and Hop Limit value for all outgoing packets from Citrix ADC. Default value: 255 Minimum value: 1 Maximum value: 255

ns-partition

The following operations can be performed on "ns-partition":

add| unset| switch| set| stat| unbind| bind| show| rm|

add ns partition

creates a new admin partition

Synopsis

add ns partition <partitionName>

Arguments

partitionName Name of the Partition. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

maxBandwidth Maximum bandwidth, in Kbps, that the partition can consume. A zero value indicates the bandwidth is unrestricted on the partition and it can consume up to the system limits. Default value: 10240 Minimum value: 0

maxConn Maximum number of concurrent connections that can be open in the partition. A zero value indicates no limit on number of open connections. Default value: 1024 Minimum value: 0

maxMemLimit Maximum memory, in megabytes, allocated to the partition. A zero value indicates the memory is unlimited on the partition and it can consume up to the system limits. Default value: 10 Minimum value: 0 Maximum value: 1048576

partitionMAC Special MAC address for the partition which is used for communication over shared vlans in this partition. If not specified, the MAC address is auto-generated.

Example

add partition <pname>

unset ns partition

Use this command to remove ns partition settings.Refer to the set ns partition command for meanings of the arguments.

Synopsis

unset ns partition <partitionName>

switch ns partition

switches to a new admin partition.

Synopsis

switch ns partition <partitionName> (-force | -save)

Arguments

partitionName Name of the Partition. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

force Switches to new admin partition without prompt for saving configuration. Configuration will not be saved

save Switches to new admin partition without prompt for saving configuration. Configuration will be saved

Example

switch partition <pname>

set ns partition

set the properties of partition

Synopsis

set ns partition <partitionName>

Arguments

partitionName Name of the Partition. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

maxBandwidth Maximum bandwidth, in Kbps, that the partition can consume. A zero value indicates the bandwidth is unrestricted on the partition and it can consume up to the system limits. Default value: 10240 Minimum value: 0

maxConn Maximum number of concurrent connections that can be open in the partition. A zero value indicates no limit on number of open connections. Default value: 1024 Minimum value: 0

maxMemLimit Maximum memory, in megabytes, allocated to the partition. A zero value indicates the memory is unlimited on the partition and it can consume up to the system limits. Default value: 10 Minimum value: 0 Maximum value: 1048576

partitionMAC Special MAC address for the partition which is used for communication over shared vlans in this partition. If not specified, the MAC address is auto-generated.

Example

set partition <pname>

stat ns partition

Displays statistics that have been collected for the specific partition.

Synopsis

stat ns partition

Arguments

partitionName Name of the partition.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Maximum Bandwidth (MaxBW) Maximum Banwidth allowed for the partition.

Maximum Connection (MaxConn) Maximum Connection allowed for the partition.

Maximum Memory (MaxMem) Maximum memory limit for the partition.

Current Bandwith (CurBW) Current Bandwidth usage for the partition.

Current Connections (CurConn) Current Connections on this partition.

Memory Usage(%) (MemUsgPcnt) Memory usage(%) on this partition.

Total Packet Drops (TotDrops) Total packet drops for the partition.

Total Drops(KB) (TotTokenDrops) Total drops(KB) for the partition.

Total Connection Drops (TotConnDrops) Total connection drops for the partition.

Related Commands

- stat ns trafficDomain

unbind ns partition

Unbind resources to a partition.

Synopsis

unbind ns partition <partitionName> (-vlan <positive_integer> | -vxlan <positive_integer> | -bridgegroup <positive_integer>)

Arguments

partitionName Name of the Partition. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

vlan Vlan Identifier. Minimum value: 1 Maximum value: 4094

vxlan VXLAN Identifier. Minimum value: 1 Maximum value: 16777215

bridgegroup Bridge group Identifier. Minimum value: 1 Maximum value: 1000

Example

unbind partition <name> -vlan 2

bind ns partition

bind resources to a partition.

Synopsis

bind ns partition <partitionName> (-vlan <positive_integer> | -vxlan <positive_integer> | -bridgegroup <positive_integer>)

Arguments

partitionName Name of the Partition. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

vlan Vlan Identifier. Minimum value: 1 Maximum value: 4094

vxlan VXLAN Identifier. Minimum value: 1 Maximum value: 16777215

bridgegroup Bridge group Identifier. Minimum value: 1 Maximum value: 1000

Example

bind partition <name> -vlan 2

show ns partition

Display all the partitions configured

Synopsis

show ns partition

Arguments

partitionName Name of partition for which to display parameters.

Output

partitionid Partition Id

partitionType Type of the Partition

maxBandwidth Maximum bandwidth, in Kbps, that the partition can consume. A zero value indicates the bandwidth is unrestricted on the partition and it can consume up to the system limits.

minBandwidth Minimum bandwidth, in Kbps, that the partition can consume. A zero value indicates the bandwidth is unrestricted on the partition and it can consume up to the system limits

maxConn Maximum number of concurrent connections that can be open in the partition. A zero value indicates no limit on number of open connections.

maxMemLimit Maximum memory, in megabytes, allocated to the partition. A zero value indicates the memory is unlimited on the partition and it can consume up to the system limits.

stateflag Used internally for display.

vlan Identifier of the vlan that is assigned to this partition.

vxlan Identifier of the vxlan that is assigned to this partition.

bridgegroup Identifier of the bridge group that is assigned to this partition.

partitionMAC Special MAC address for the partition which is used for communication over shared vlans in this partition. If not specified, the MAC address is auto-generated.

pmacInternal Partition MAC is generated internally.

devno count

Example

show partition

rm ns partition

deletes a admin partition

Synopsis

rm ns partition <partitionName>

Arguments

partitionName Name of the Partition. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

Example

rm partition <pname>

ns-partitionMAC

The following operations can be performed on "ns-partitionMAC":

show ns partitionMAC

Display all configured MACs for partitions

Synopsis

show ns partitionMAC

Arguments

Output

partitionMAC A configured virtual MAC address that can be used by a partition for communication over shared VLANs.

partitionName Name of the partition to which the MAC has been assigned.

devno count stateflag

Example

show ns partitionMAC

ns-pbr

The following operations can be performed on "ns-pbr":

add| disable| rm| unset| show| stat| enable| set|

add ns pbr

Adds a policy based route (PBR) to the Citrix ADC. To commit this operation, you must apply the PBRs. A PBR specifies criteria for selecting outgoing IPv4 packets and, typically, a next hop to which to send the selected packets. For example, you can configure the Citrix ADC to route outgoing packets from a specific IP address or range to a particular next hop router.

Note: The Citrix ADC process PBRs before processing the RNAT rules.

Synopsis

add ns pbr <name> <action> [-srcIP <srcIPVal>] [-srcPort <srcPortVal>] [-destIP <destIPVal>] [-destPort <destPortVal>] ((-nextHop <nextHopVal>) | (-ipTunnel <ipTunnelName>)) [-srcMac <mac_addr>] [-msr (ENABLED | DISABLED)]

Arguments

name Name for the PBR. Must begin with an ASCII alphabetic or underscore \(_\) character, and must contain only ASCII alphanumeric, underscore, hash \(#\), period \(.\), space, colon \(:\), at \(@\), equals \(=\), and hyphen \(-\) characters. Cannot be changed after the PBR is created.

action Action to perform on the outgoing IPv4 packets that match the PBR.

Available settings function as follows:

- ALLOW - The Citrix ADC sends the packet to the designated next-hop router.
- DENY - The Citrix ADC applies the routing table for normal destination-based routing.

Possible values: ALLOW, DENY

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

srcIP IP address or range of IP addresses to match against the source IP address of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

srcIPVal IP address or range of IP addresses to match against the source IP address of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.

srcPort Port number or range of port numbers to match against the source port number of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

srcPortVal Port number or range of port numbers to match against the source port number of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols. Maximum value: 65535

destIP IP address or range of IP addresses to match against the destination IP address of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

destIPVal IP address or range of IP addresses to match against the destination IP address of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.

destPort Port number or range of port numbers to match against the destination port number of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

destPortVal Port number or range of port numbers to match against the destination port number of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols. Maximum value: 65535

nextHop IP address of the next hop router or the name of the link load balancing virtual server to which to send matching packets if action is set to ALLOW. If you specify a link load balancing (LLB) virtual server, which can provide a backup if a next hop link fails, first make sure that the next hops bound to the LLB virtual server are actually next hops that are directly connected to the Citrix ADC. Otherwise, the Citrix ADC throws an error when you attempt to create the PBR. The next hop can be null to represent null routes

nextHopVal The Next Hop IP address or gateway name.

ipTunnel The Tunnel name.

ipTunnelName The iptunnel name where packets need to be forwarded upon.

vxlanVlanMap The vlan to vxlan mapping to be applied for incoming packets over this pbr tunnel

srcMac MAC address to match against the source MAC address of an outgoing IPv4 packet.

srcMacMask Used to define range of Source MAC address. It takes string of 0 and 1, 0s are for exact match and 1s for wildcard. For matching first 3 bytes of MAC address, srcMacMask value "000000111111". Default value: "000000000000"

protocol Protocol, identified by protocol name, to match against the protocol of an outgoing IPv4 packet.

Possible values: ICMP, IGMP, TCP, EGP, IGP, ARGUS, UDP, RDP, RSVP, EIGRP, L2TP, ISIS, GGP, IPoverIP, ST, CBT, BBN-RCC-M, NVP-II, PUP, EMCON, XNET, CHAOS, MUX, DCN-MEAS, HMP, PRM, XNS-IDP, TRUNK-1, TRUNK-2, LEAF-1, LEAF-2, IRTP, ISO-TP4, NETBLT, MFE-NSP, MERIT-INP, SEP, 3PC, IDPR, XTP, DDP, IDPR-CMTP, TP++, IL, IPv6, SDRP, IPv6-Route, IPv6-Frag, IDRP, GRE, MHRP, BNA, ESP, AH, I-NLSP, SWIPE, NARP, MOBILE, TLSP, SKIP, ICMPV6, IPv6-NoNx, IPv6-Opts, Any-Host-Internal-Protocol, CFTP, Any-Local-Network, SAT-EXPAK, KRYPTOLAN, RVD, IPPC, Any-Distributed-File-System, TFTP, VISA, IPCV, CPNX, CPHB, WSN, PVP, BR-SAT-MO, SUN-ND, WB-MON, WB-EXPAK, ISO-IP, VMTP, SECURE-VM, VINES, TTP, NSFNET-IG, DGP, TCF, OSPFIGP, Sprite-RP, LARP, MTP, AX.25, IPIP, MICP, SCC-SP, ETHERIP, Any-Private-Encryption-Scheme, GMTP, IFMP, PNNI, PIM, ARIS, SCPS, QNX, A/N, IPComp, SNP, Compaq-Pe, IPX-in-IP, VRRP, PGM, Any-0-Hop-Protocol, ENCAP, DDX, IATP, STP, SRP, UTI, SMP, SM, PTP, FIRE, CRTP, CRUDP, SSCOPMCE, IPLT, SPS, PIPE, SCTP, FC, RSVP-E2E-IGNORE, Mobility-Header, UDPLite

protocolNumber Protocol, identified by protocol number, to match against the protocol of an outgoing IPv4 packet. Minimum value: 1 Maximum value: 255

vlan ID of the VLAN. The Citrix ADC compares the PBR only to the outgoing packets on the specified VLAN. If you do not specify any interface ID, the appliance compares the PBR to the outgoing packets on all VLANs. Minimum value: 1 Maximum value: 4094

vxlan ID of the VXLAN. The Citrix ADC compares the PBR only to the outgoing packets on the specified VXLAN. If you do not specify any interface ID, the appliance compares the PBR to the outgoing packets on all VXLANs. Minimum value: 1 Maximum value: 16777215

interface ID of an interface. The Citrix ADC compares the PBR only to the outgoing packets on the specified interface. If you do not specify any value, the appliance compares the PBR to the outgoing packets on all interfaces.

priority Priority of the PBR, which determines the order in which it is evaluated relative to the other PBRs. If you do not specify priorities while creating PBRs, the PBRs are evaluated in the order in which they are created. Minimum value: 1 Maximum value: 81920

msr Monitor the route specified byte Next Hop parameter. This parameter is not applicable if you specify a link load balancing (LLB) virtual server name with the Next Hop parameter.

Possible values: ENABLED, DISABLED Default value: DISABLED

monitor The name of the monitor.(Can be only of type ping or ARP)

state Enable or disable the PBR. After you apply the PBRs, the Citrix ADC compares outgoing packets to the enabled PBRs.

Possible values: ENABLED, DISABLED Default value: ENABLED

ownerGroup The owner node group in a Cluster for this pbr rule. If ownernode is not specified then the pbr rule is treated as Striped pbr rule. Default value: DEFAULT_NG

Example

add ns pbr a allow -srcip 10.102.37.252 -destip 10.10.10.2 -nexthop 11.11.11.2 add ns pbr pt ALLOW -srcIP = 20.1.4.1 -destIP = 20.1.4.3 -ipTunnel t206 -vlanVxlanMap p3

Related Commands

- apply pbrs

disable ns pbr

Disables a PBR. To commit this operation, you must apply the PBRs. After you apply the PBRs, the Citrix ADC does not compare outgoing packets against the disabled PBRs

Synopsis

disable ns pbr <name> ...

Arguments

name Name of PBR that you want to disable.

Example

disable ns pbr foo

Related Commands

- clear pbrs

rm ns pbr

Removes a PBR from the Citrix ADC. To commit this operation, you must apply the PBRs.

Synopsis

rm ns pbr <name> ...

Arguments

name Name of the PBR that you want to remove.

Example

rm ns pbr a

Related Commands

- clear pbrs

unset ns pbr

Resets the attributes of the specified PBR. Attributes for which a default value is available revert to their default values. Refer to the set ns pbr command for descriptions of the parameters..Refer to the set ns pbr command for meanings of the arguments.

Synopsis

unset ns pbr <name>

Example

unset ns pbr rule1 -srcPort

Related Commands

- apply pbrs

show ns pbr

Displays settings related to the PBRs. To display settings of all the PBRs, run the command without any parameters. To display settings of a particular PBR, specify the name of the PBR.

Synopsis

show ns pbr

Arguments

name Name of the PBR whose details you want the Citrix ADC to display.

detail To get a detailed view.

Output

action Action to perform on the outgoing IPv4 packets that match the PBR.

Available settings function as follows:

- ALLOW - The Citrix ADC sends the packet to the designated next-hop router.
- DENY - The Citrix ADC applies the routing table for normal destination-based routing.

srcMac MAC address to match against the source MAC address of an outgoing IPv4 packet.

srcMacMask Used to define range of Source MAC address. It takes string of 0 and 1, 0s are for exact match and 1s for wildcard. For matching first 3 bytes of MAC address, srcMacMask value "000000111111".

protocol The protocol number in IP header or name.

protocolNumber The protocol number in IP header or name.

srcPortVal Port number or range of port numbers to match against the source port number of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols.

operator Either the equals (=) or does not equal (!=) logical operator.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

destPortVal Port number or range of port numbers to match against the destination port number of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols.

operator Either the equals (=) or does not equal (!=) logical operator.

srcIPVal IP address or range of IP addresses to match against the source IP address of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.

operator Either the equals (=) or does not equal (!=) logical operator.

destIPVal IP address or range of IP addresses to match against the destination IP address of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.

operator Either the equals (=) or does not equal (!=) logical operator.

vlan ID of the VLAN. The Citrix ADC compares the PBR only to the outgoing packets on the specified VLAN. If you do not specify any interface ID, the appliance compares the PBR to the outgoing packets on all VLANs.

vxlan ID of the VXLAN. The Citrix ADC compares the PBR only to the outgoing packets on the specified VXLAN. If you do not specify any interface ID, the appliance compares the PBR to the outgoing packets on all VXLANs.

state Enable or disable the PBR. After you apply the PBRs, the Citrix ADC compares outgoing packets to the enabled PBRs.

interface ID of an interface. The Citrix ADC compares the PBR only to the outgoing packets on the specified interface. If you do not specify any value, the appliance compares the PBR to the outgoing packets on all interfaces.

hits The hits of this PBR.

priority Priority of the PBR, which determines the order in which it is evaluated relative to the other PBRs. If you do not specify priorities while creating PBRs, the PBRs are evaluated in the order in which they are created.

kernelstate The commit status of the PBR.

nextHopVal The Next Hop IP address or gateway name.

ipTunnelName The iptunnel name where packets need to be forwarded upon.

vxlanVlanMap The vlan to vxlan mapping to be applied for incoming packets over this pbr tunnel

msr Whether Monitored Static Route(MSR) is enabled or disabled.

monitor Name of the monitor, of type PING or ARP, configured on the Citrix ADC to monitor the route specified by the Next Hop parameter. You must enable the MSR parameter before setting this parameter.

state If this route is UP/DOWN.

totalprobes The total number of probes sent.

totalfailedprobes The total number of failed probes.

failedprobes Number of the current failed monitoring probes.

monStatCode The code indicating the monitor response.

monStatParam1 First parameter for use with message code.

monStatParam2 Second parameter for use with message code.

monStatParam3 Third parameter for use with message code.

data Internal data of this route.

ownerGroup The owner node group in a Cluster for this pbr rule. If ownernode is not specified then the pbr rule is treated as Striped pbr rule.

devno count stateflag

Example

show ns pbr a Name: a Action: ALLOW Hits: 0 srcIP = 10.102.37.252 destIP = 10.10.10.2 srcMac: srcMacMask: Protocol: Vlan: Interface: Active Status: ENABLED Applied Status: NOTAPPLIED Priority: 10 NextHop: 11.11.11.2

stat ns pbr

Displays statistics related to the PBRs. To display statistics of all the PBRs, run the command without any parameters. To display statistics of a particular PBR, specify the name of the PBR.

Synopsis

stat ns pbr

Arguments

name Name of the PBR whose statistics you want the Citrix ADC to display.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Allow PBR hits (PBRAllow) Total packets that matched the PBR (Policy-Based Routes) with action ALLOW

Deny PBR hits (PBRDeny) Total packets that matched the PBR with action DENY

PBR hits (PBRTotHits) Total packets that matched one of the configured PBR

PBR misses (PBRMiss) Total packets that did not match any PBR

PBR Null Drop (PBRNullDrop) Total packets that are dropped due to null nexthop

Hits for this PBR (PBRHits) Number of times the pbr was hit

Example

stat pbr

Related Commands

- stat ns partition

enable ns pbr

Enables a PBR. To commit this operation, you must apply the PBRs. After you apply the PBRs, the Citrix ADC compares outgoing packets to the enabled PBRs.

Synopsis

enable ns pbr <name> ...

Arguments

name Name of PBR that you want to enable.

Example

enable ns pbr foo

Related Commands

- clear pbrs

set ns pbr

Modifies the specified parameters of a PBR. To commit this operation, you must apply the PBRs.

Synopsis

set ns pbr <name> [-srcIP <srcIPVal>] [-srcPort <srcPortVal>] [-destIP <destIPVal>] [-destPort <destPortVal>] ((-nextHop <nextHopVal>) | (-ipTunnel <ipTunnelName>)) [-srcMac <mac_addr>] [-msr (ENABLED | DISABLED)]

Arguments

name Name of the PBR whose parameters you want to modify.

action Action to perform on the outgoing IPv4 packets that match the PBR.

Available settings function as follows:

- ALLOW - The Citrix ADC sends the packet to the designated next-hop router.
- DENY - The Citrix ADC applies the routing table for normal destination-based routing.

Possible values: ALLOW, DENY

srcIP IP address or range of IP addresses to match against the source IP address of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

srcIPVal IP address or range of IP addresses to match against the source IP address of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.

srcPort Port number or range of port numbers to match against the source port number of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

srcPortVal Port number or range of port numbers to match against the source port number of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols. Maximum value: 65535

destIP IP address or range of IP addresses to match against the destination IP address of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

destIPVal IP address or range of IP addresses to match against the destination IP address of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.

destPort Port number or range of port numbers to match against the destination port number of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

destPortVal Port number or range of port numbers to match against the destination port number of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols. Maximum value: 65535

nextHop IP address of the next hop router or the name of the link load balancing virtual server to which to send matching packets if action is set to ALLOW. If you specify a link load balancing (LLB) virtual server, which can provide a backup if a next hop link fails, first make sure that the next hops

bound to the LLB virtual server are actually next hops that are directly connected to the Citrix ADC. Otherwise, the Citrix ADC throws an error when you attempt to create the PBR. The next hop can be null to represent null routes

nextHopVal The Next Hop IP address or gateway name.

ipTunnel The Tunnel name.

ipTunnelName The iptunnel name where packets need to be forwarded upon.

vxlanVlanMap The vlan to vxlan mapping to be applied for incoming packets over this pbr tunnel

srcMac MAC address to match against the source MAC address of an outgoing IPv4 packet.

srcMacMask Used to define range of Source MAC address. It takes string of 0 and 1, 0s are for exact match and 1s for wildcard. For matching first 3 bytes of MAC address, srcMacMask value "000000111111". Default value: "000000000000"

protocol Protocol, identified by protocol name, to match against the protocol of an outgoing IPv4 packet.

Possible values: ICMP, IGMP, TCP, EGP, IGP, ARGUS, UDP, RDP, RSVP, EIGRP, L2TP, ISIS, GGP, IPoverIP, ST, CBT, BBN-RCC-M, NVP-II, PUP, EMCON, XNET, CHAOS, MUX, DCN-MEAS, HMP, PRM, XNS-IDP, TRUNK-1, TRUNK-2, LEAF-1, LEAF-2, IRTP, ISO-TP4, NETBLT, MFE-NSP, MERIT-INP, SEP, 3PC, IDPR, XTP, DDP, IDPR-CMTP, TP++, IL, IPv6, SDRP, IPv6-Route, IPv6-Frag, IDRP, GRE, MHRP, BNA, ESP, AH, I-NLSP, SWIPE, NARP, MOBILE, TLSP, SKIP, ICMPV6, IPv6-NoNx, IPv6-Opts, Any-Host-Internal-Protocol, CFTP, Any-Local-Network, SAT-EXPAK, KRYPTOLAN, RVD, IPPC, Any-Distributed-File-System, TFTP, VISA, IPCV, CPNX, CPHB, WSN, PVP, BR-SAT-MO, SUN-ND, WB-MON, WB-EXPAK, ISO-IP, VMTP, SECURE-VM, VINES, TTP, NSFNET-IG, DGP, TCF, OSPFIGP, Sprite-RP, LARP, MTP, AX.25, IPIP, MICP, SCC-SP, ETHERIP, Any-Private-Encryption-Scheme, GMTP, IFMP, PNNI, PIM, ARIS, SCPS, QNX, A/N, IPComp, SNP, Compaq-Pe, IPX-in-IP, VRRP, PGM, Any-0-Hop-Protocol, ENCAP, DDX, IATP, STP, SRP, UTI, SMP, SM, PTP, FIRE, CRTP, CRUDP, SSCOPMCE, IPLT, SPS, PIPE, SCTP, FC, RSVP-E2E-IGNORE, Mobility-Header, UDPLite

protocolNumber Protocol, identified by protocol number, to match against the protocol of an outgoing IPv4 packet. Minimum value: 1 Maximum value: 255

vlan ID of the VLAN. The Citrix ADC compares the PBR only to the outgoing packets on the specified VLAN. If you do not specify any interface ID, the appliance compares the PBR to the outgoing packets on all VLANs. Minimum value: 1 Maximum value: 4094

vxlan ID of the VXLAN. The Citrix ADC compares the PBR only to the outgoing packets on the specified VXLAN. If you do not specify any interface ID, the appliance compares the PBR to the outgoing packets on all VXLANs. Minimum value: 1 Maximum value: 16777215

interface ID of an interface. The Citrix ADC compares the PBR only to the outgoing packets on the specified interface. If you do not specify any value, the appliance compares the PBR to the outgoing packets on all interfaces.

priority Priority of the PBR, which determines the order in which it is evaluated relative to the other PBRs. If you do not specify priorities while creating PBRs, the PBRs are evaluated in the order in which they are created. Minimum value: 1 Maximum value: 81920

msr Monitor the route specified byte Next Hop parameter. This parameter is not applicable if you specify a link load balancing (LLB) virtual server name with the Next Hop parameter.

Possible values: ENABLED, DISABLED Default value: DISABLED

monitor Name of the monitor, of type PING or ARP, configured on the Citrix ADC to monitor the route specified by the Next Hop parameter. You must enable the MSR parameter before setting this parameter.

Example

set ns pbr a -srcPort 50

Related Commands

- apply pbrs

ns-pbr6

The following operations can be performed on "ns-pbr6":

unset| clear| set| show| stat| disable| apply| rm| enable| renumber| add|

unset ns pbr6

Resets the attributes of the specified PBR6. Attributes for which a default value is available revert to their default values. Refer to the set ns pbr6 command for descriptions of the parameters..Refer to the set ns pbr6 command for meanings of the arguments.

Synopsis

unset ns pbr6 <name>

Example

unset ns pbr6 rule1 -srcPort

clear ns pbr6

Removes all PBR6s from the Citrix ADC. This operation does not require an explicit apply.

Synopsis

clear ns pbr6

Example

clear ns pbr6

set ns pbr6

Modifies the specified parameters of a PBR6.To commit this operation, you must apply the PBR6s.

Synopsis

set ns pbr6 <name> [-srcIPv6 <srcIPv6Val>] [-srcPort <srcPortVal>] [-destIPv6 <destIPv6Val>] [-destPort <destPortVal>] [-srcMac <mac_addr>] [-msr (ENABLED | DISABLED)] [(-nextHop <nextHopVal>) | (-ipTunnel <string>)]

Arguments

name Name of the PBR6 whose parameters you want to modify.

action Action to perform on the outgoing IPv6 packets that match the PBR6.

Available settings function as follows:

- ALLOW - The Citrix ADC sends the packet to the designated next-hop router.
- DENY - The Citrix ADC applies the routing table for normal destination-based routing.

Possible values: ALLOW, DENY

srcIPv6 IP address or range of IP addresses to match against the source IP address of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

srcIPv6Val IP address or range of IP addresses to match against the source IP address of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen.

srcPort Source Port (range).

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

srcPortVal Port number or range of port numbers to match against the source port number of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen. For example: 40-90. Maximum value: 65535

destIPv6 IP address or range of IP addresses to match against the destination IP address of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

destIPv6Val IP address or range of IP addresses to match against the destination IP address of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen.

destPort Destination Port (range).

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

destPortVal Port number or range of port numbers to match against the destination port number of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols. Maximum value: 65535

srcMac MAC address to match against the source MAC address of an outgoing IPv6 packet.

srcMacMask Used to define range of Source MAC address. It takes string of 0 and 1, 0s are for exact match and 1s for wildcard. For matching first 3 bytes of MAC address, srcMacMask value "000000111111". Default value: "000000000000"

protocol Protocol, identified by protocol name, to match against the protocol of an outgoing IPv6 packet.

Possible values: ICMPV6, TCP, UDP, ICMP, IGMP, EGP, IGP, ARGUS, RDP, RSVP, EIGRP, L2TP, ISIS, GGP, IPoverIP, ST, CBT, BBN-RCC-M, NVP-II, PUP, EMCON, XNET, CHAOS, MUX, DCN-MEAS, HMP, PRM, XNS-IDP, TRUNK-1, TRUNK-2, LEAF-1, LEAF-2, IRTP, ISO-TP4, NETBLT, MFE-NSP, MERIT-INP, SEP, 3PC, IDPR, XTP, DDP, IDPR-CMTP, TP++, IL, IPv6, SDRP, IPv6-Route, IPv6-Frag, IDRP, GRE, MHRP, BNA, ESP, AH, I-NLSP, SWIPE, NARP, MOBILE, TLSP, SKIP, IPv6-NoNx, IPv6-Opts, Any-Host-Internal-Protocol, CFTP, Any-Local-Network, SAT-EXPAK, KRYPTOLAN, RVD, IPPC, Any-Distributed-File-System, TFTP, VISA, IPCV, CPNX, CPHB, WSN, PVP, BR-SAT-MO, SUN-ND, WB-MON, WB-EXPAK, ISO-IP, VMTP, SECURE-VM, VINES, TTP, NSFNET-IG, DGP, TCF, OSPFIGP, Sprite-RP, LARP, MTP, AX.25, IPIP, MICP, SCC-SP, ETHERIP, Any-Private-Encryption-Scheme, GMTP, IFMP, PNNI, PIM, ARIS, SCPS, QNX, A/N, IPComp, SNP, Compaq-Pe, IPX-in-IP, VRRP, PGM, Any-0-Hop-Protocol, ENCAP, DDX, IATP, STP, SRP, UTI, SMP, SM, PTP, FIRE, CRTP, CRUDP, SSCOPMCE, IPLT, SPS, PIPE, SCTP, FC, RSVP-E2E-IGNORE, Mobility-Header, UDPLite

protocolNumber Protocol, identified by protocol number, to match against the protocol of an outgoing IPv6 packet. Minimum value: 1 Maximum value: 255

vlan ID of the VLAN. The Citrix ADC compares the PBR6 only to the outgoing packets on the specified VLAN. If you do not specify an interface ID, the appliance compares the PBR6 to the outgoing packets on all VLANs. Minimum value: 1 Maximum value: 4094

vxlan ID of the VXLAN. The Citrix ADC compares the PBR6 only to the outgoing packets on the specified VXLAN. If you do not specify an interface ID, the appliance compares the PBR6 to the outgoing packets on all VXLANs. Minimum value: 1 Maximum value: 16777215

interface ID of an interface. The Citrix ADC compares the PBR6 only to the outgoing packets on the specified interface. If you do not specify a value, the appliance compares the PBR6 to the outgoing packets on all interfaces.

priority Priority of the PBR6, which determines the order in which it is evaluated relative to the other PBR6s. If you do not specify priorities while creating PBR6s, the PBR6s are evaluated in the order in which they are created. Minimum value: 1 Maximum value: 81920

msr Monitor the route specified by the Next Hop parameter.

Possible values: ENABLED, DISABLED Default value: DISABLED

monitor The name of the monitor.(Can be only of type ping or ARP)

nextHop IP address of the next hop router to which to send matching packets if action is set to ALLOW. This next hop should be directly reachable from the appliance.

nextHopVal The Next Hop IPv6 address

ipTunnel The iptunnel name where packets need to be forwarded upon.

vxlanVlanMap The vlan to vxlan mapping to be applied for incoming packets over this pbr tunnel.

nextHopVlan VLAN number to be used for link local nexthop . Minimum value: 1 Maximum value: 4094

Example

set ns pbr6 rule1 -srcPort 50

show ns pbr6

Displays settings related to the PBR6s. To display settings of all the PBR6s, run the command without any parameters. To display settings of a particular PBR6, specify the name of the PBR6.

Synopsis

show ns pbr6

Arguments

name Name of the PBR6 whose settings you want the Citrix ADC to display.

detail To get a detailed view.

Output

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

action Action to perform on the outgoing IPv6 packets that match the PBR6.

Available settings function as follows:

- ALLOW - The Citrix ADC sends the packet to the designated next-hop router.
- DENY - The Citrix ADC applies the routing table for normal destination-based routing.

srcMac MAC address to match against the source MAC address of an outgoing IPv6 packet.

srcMacMask Used to define range of Source MAC address. It takes string of 0 and 1, 0s are for exact match and 1s for wildcard. For matching first 3 bytes of MAC address, srcMacMask value "000000111111".

stateflag PBR6 state flag.

protocol Protocol number in IPv6 header or name.

protocolNumber Protocol number in IPv6 header or name.

srcPortVal Port number or range of port numbers to match against the source port number of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

operator Either the equals (=) or does not equal (!=) logical operator.

destPortVal Port number or range of port numbers to match against the destination port number of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols.

operator Either the equals (=) or does not equal (!=) logical operator.

srcIPv6Val IP address or range of IP addresses to match against the source IP address of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen.

operator Either the equals (=) or does not equal (!=) logical operator.

destIPv6Val IP address or range of IP addresses to match against the destination IP address of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen.

operator Either the equals (=) or does not equal (!=) logical operator.

vlan ID of the VLAN. The Citrix ADC compares the PBR6 only to the outgoing packets on the specified VLAN. If you do not specify an interface ID, the appliance compares the PBR6 to the outgoing packets on all VLANs.

vxlan ID of the VXLAN. The Citrix ADC compares the PBR6 only to the outgoing packets on the specified VXLAN. If you do not specify an interface ID, the appliance compares the PBR6 to the outgoing packets on all VXLANs.

state Enable or disable the PBR6. After you apply the PBR6s, the Citrix ADC compares outgoing packets to the enabled PBR6s.

kernelstate Commit status of the PBR6.

interface ID of an interface. The Citrix ADC compares the PBR6 only to the outgoing packets on the specified interface. If you do not specify a value, the appliance compares the PBR6 to the outgoing packets on all interfaces.

hits Number of hits of this PBR6.

priority Priority of the PBR6, which determines the order in which it is evaluated relative to the other PBR6s. If you do not specify priorities while creating PBR6s, the PBR6s are evaluated in the order in which they are created.

msr Whether Monitored Static Route(MSR) is enabled or disabled.

monitor Name of the monitor, of type PING6 or ARP, configured on the Citrix ADC to monitor the route specified by the Next Hop parameter. You must enable the MSR parameter before setting the Monitor parameter.

state If this route is UP/DOWN.

totalprobes The total number of probes sent.

totalfailedprobes The total number of failed probes.

failedprobes Number of the current failed monitoring probes.

monStatCode The code indicating the monitor response.

monStatParam1 First parameter for use with message code.

monStatParam2 Second parameter for use with message code.

monStatParam3 Third parameter for use with message code.

nextHopVal ID of the VLAN, if you have specified a link local address for the Next Hop parameter.

ipTunnel The iptunnel name where packets need to be forwarded upon.

vxlanVlanMap The vlan to vxlan mapping to be applied for incoming packets over this pbr tunnel.

nextHopVlan VLAN number to be used for link local nexthop .

data Internal data of this route.

ownerGroup The owner node group in a Cluster for this pbr rule. If owner node group is not specified then the pbr rule is treated as Striped pbr rule.

devno count

Example

show ns pbr6 rule1 1)

```
    Name: r1                            Action: DENY

    srcIPv6 = 2001::1

    destIPv6

    srcMac:                             srcMacMask:

    Protocol:

    Vlan:                               Interface:

    Active Status: ENABLED              Applied Status: NOTAPPLIED

    Priority: 10                        Hits: 0

    Nexthop:
```

stat ns pbr6

Displays statistics related to the PBR6s. To display statistics of all the PBR6s, run the command without any parameters. To display statistics of a particular PBR6, specify the name of the PBR6.

Synopsis

stat ns pbr6

Arguments

name Name of the PBR6 whose statistics you want the Citrix ADC to display.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Allow PBR6 hits (PBR6Allow) Total packets that matched the PBR6 with action ALLOW

Deny PBR6 hits (PBR6Deny) Total packets that matched PBR6 with action DENY

PBR6 hits (PBR6TotHits) Total packets that matched one of the configured PBR6

PBR6 misses (PBR6Miss) Total packets that did not match any PBR6

PBR6 Null Drop (PBR6NullDrop) Total packets that are dropped due to null next hop

Hits for this PBR6 (PBR6Hits) Number of times the pbr6 was hit

Example

stat pbr6

Related Commands

- stat ns partition

disable ns pbr6

Disables a PBR6. To commit this operation, you must apply the PBR6s.After you apply the PBR6s, the Citrix ADC does not compare outgoing packets to the disabled PBR6s.

Synopsis

disable ns pbr6 <name> ...

Arguments

name Name of PBR6 that you want to disable.

Example

disable ns pbr6 rule1

apply ns pbr6

Updates the PBR6's memory tree (lookup table), adding any new PBR6 and applying any modifications to the existing PBR6s. The lookup table includes the configuration of all the extended PBR6s on the Citrix ADC. The Citrix ADC appliance uses the lookup table (not the configuration file) to filter the outgoing IPv6 packets.

Synopsis

apply ns pbr6

Arguments

Example

apply ns pbr6

rm ns pbr6

Removes a PBR6 from the Citrix ADC. To commit this operation, you must apply the PBR6s.

Synopsis

rm ns pbr6 <name> ...

Arguments

name Name of the PBR6 that you want to remove.

Example

rm ns pbr6 rule1

enable ns pbr6

Enables a PBR6. To commit this operation, you must apply the PBR6s.After you apply the PBR6s, the Citrix ADC compares outgoing packets to the enabled PBR6.

Synopsis

enable ns pbr6 <name> ...

Arguments

name Name of PBR6 that you want to enable.

Example

enable ns pbr6 rule1

renumber ns pbr6

Renumbers the priorities of PBR6s to multiples of 10.To commit this operation, you must apply the PBR6s. Enables you to assign a new PBR6 a priority that is between two existing, consecutively numbered priorities. For example, if two PBR6s, PBR6-1 and PBR6-2, have priorities 2 and 3 renumbering changes those priorities to 20 and 30. You can then add PBR6-3 with priority 25.

Synopsis

renumber ns pbr6

Example

renumber pbr6

add ns pbr6

Adds an IPv6 policy based route (PBR6) to the Citrix ADC. To commit this operation, you must apply the PBR6s. A PBR6 specifies criteria for selecting outgoing IPv6 packets and, typically, a next hop to which to send the selected packets. For example, you can configure the Citrix ADC to route outgoing packets from a specific IP address or range to a particular next hop router.

Note: The Citrix ADC process PBR6s before processing the RNAT rules.

Synopsis

add ns pbr6 <name> <action> [-srcIPv6 <srcIPv6Val>] [-srcPort <srcPortVal>] [-destIPv6 <destIPv6Val>] [-destPort <destPortVal>] [-srcMac <mac_addr>] [-msr (ENABLED | DISABLED)] [(-nextHop <nextHopVal>) | (-ipTunnel <string>)]

Arguments

name Name for the PBR6. Must begin with an ASCII alphabetic or underscore \(_\) character, and must contain only ASCII alphanumeric, underscore, hash \(#\), period \(.\), space, colon \(:\), at \(@\), equals \(=\), and hyphen \(-\) characters. Cannot be changed after the PBR6 is created.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

action Action to perform on the outgoing IPv6 packets that match the PBR6.

Available settings function as follows:

- ALLOW - The Citrix ADC sends the packet to the designated next-hop router.
- DENY - The Citrix ADC applies the routing table for normal destination-based routing.

Possible values: ALLOW, DENY

srcIPv6 IP address or range of IP addresses to match against the source IP address of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

srcIPv6Val IP address or range of IP addresses to match against the source IP address of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen.

srcPort Port number or range of port numbers to match against the source port number of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

srcPortVal Source port (range). Maximum value: 65535

destIPv6 IP address or range of IP addresses to match against the destination IP address of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

destIPv6Val IP address or range of IP addresses to match against the destination IP address of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen.

destPort Port number or range of port numbers to match against the destination port number of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.

Note: The destination port can be specified only for TCP and UDP protocols.

operator Either the equals (=) or does not equal (!=) logical operator.

Possible values: =, !=, EQ, NEQ

destPortVal Destination port (range). Maximum value: 65535

srcMac MAC address to match against the source MAC address of an outgoing IPv6 packet.

srcMacMask Used to define range of Source MAC address. It takes string of 0 and 1, 0s are for exact match and 1s for wildcard. For matching first 3 bytes of MAC address, srcMacMask value "000000111111". Default value: "000000000000"

protocol Protocol, identified by protocol name, to match against the protocol of an outgoing IPv6 packet.

Possible values: ICMPV6, TCP, UDP, ICMP, IGMP, EGP, IGP, ARGUS, RDP, RSVP, EIGRP, L2TP, ISIS, GGP, IPoverIP, ST, CBT, BBN-RCC-M, NVP-II, PUP, EMCON, XNET, CHAOS, MUX, DCN-MEAS, HMP, PRM, XNS-IDP, TRUNK-1, TRUNK-2, LEAF-1, LEAF-2, IRTP, ISO-TP4, NETBLT, MFE-NSP, MERIT-INP, SEP, 3PC, IDPR, XTP, DDP, IDPR-CMTP, TP++, IL, IPv6, SDRP, IPv6-Route, IPv6-Frag, IDRP, GRE, MHRP, BNA, ESP, AH, I-NLSP, SWIPE, NARP, MOBILE, TLSP, SKIP, IPv6-NoNx, IPv6-Opts, Any-Host-Internal-Protocol, CFTP, Any-Local-Network, SAT-EXPAK, KRYPTOLAN, RVD, IPPC, Any-Distributed-File-System, TFTP, VISA, IPCV, CPNX, CPHB, WSN, PVP, BR-SAT-MO, SUN-ND, WB-MON, WB-EXPAK, ISO-IP, VMTP, SECURE-VM, VINES, TTP, NSFNET-IG, DGP, TCF, OSPFIGP, Sprite-RP, LARP, MTP, AX.25, IPIP, MICP, SCC-SP, ETHERIP, Any-Private-Encryption-Scheme, GMTP, IFMP, PNNI, PIM, ARIS, SCPS, QNX, A/N, IPComp, SNP, Compaq-Pe, IPX-in-IP, VRRP, PGM, Any-0-Hop-Protocol, ENCAP, DDX, IATP, STP, SRP, UTI, SMP, SM, PTP, FIRE, CRTP, CRUDP, SSCOPMCE, IPLT, SPS, PIPE, SCTP, FC, RSVP-E2E-IGNORE, Mobility-Header, UDPLite

protocolNumber Protocol, identified by protocol number, to match against the protocol of an outgoing IPv6 packet. Minimum value: 1 Maximum value: 255

vlan ID of the VLAN. The Citrix ADC compares the PBR6 only to the outgoing packets on the specified VLAN. If you do not specify an interface ID, the appliance compares the PBR6 to the outgoing packets on all VLANs. Minimum value: 1 Maximum value: 4094

vxlan ID of the VXLAN. The Citrix ADC compares the PBR6 only to the outgoing packets on the specified VXLAN. If you do not specify an interface ID, the appliance compares the PBR6 to the outgoing packets on all VXLANs. Minimum value: 1 Maximum value: 16777215

interface ID of an interface. The Citrix ADC compares the PBR6 only to the outgoing packets on the specified interface. If you do not specify a value, the appliance compares the PBR6 to the outgoing packets on all interfaces.

priority Priority of the PBR6, which determines the order in which it is evaluated relative to the other PBR6s. If you do not specify priorities while creating PBR6s, the PBR6s are evaluated in the order in which they are created. Minimum value: 1 Maximum value: 81920

state Enable or disable the PBR6. After you apply the PBR6s, the Citrix ADC compares outgoing packets to the enabled PBR6s.

Possible values: ENABLED, DISABLED Default value: ENABLED

msr Monitor the route specified by the Next Hop parameter.

Possible values: ENABLED, DISABLED Default value: DISABLED

monitor The name of the monitor.(Can be only of type ping or ARP)

nextHop IP address of the next hop router to which to send matching packets if action is set to ALLOW. This next hop should be directly reachable from the appliance.

nextHopVal The Next Hop IPv6 address.

ipTunnel The iptunnel name where packets need to be forwarded upon.

vxlanVlanMap The vlan to vxlan mapping to be applied for incoming packets over this pbr tunnel.

nextHopVlan VLAN number to be used for link local nexthop . Minimum value: 1 Maximum value: 4094

ownerGroup The owner node group in a Cluster for this pbr rule. If owner node group is not specified then the pbr rule is treated as Striped pbr rule. Default value: DEFAULT_NG

Example

add ns pbr6 rule1 ALLOW -srcport 45-1024 -destIPv6 2001::45 -nexthop 2001::49 add ns pbr6 rule2 ALLOW -srcIPv6 200::1 -destIPv6 200::5 -priority 10 -ipTunnel t8 -vxlanVlanMap maptbl1

ns-pbrs

The following operations can be performed on "ns-pbrs":

clear| renumber| apply|

clear ns pbrs

Removes all PBRs from the Citrix ADC. This operation does not require an explicit apply.

Synopsis

clear ns pbrs

Example

clear ns pbrs

renumber ns pbrs

Renumbers the priorities of PBRs to multiples of 10.To commit this operation, you must apply the PBRs. Enables you to assign a new PBR a priority that is between two existing, consecutively numbered priorities. For example, if two PBRs, PBR1 and PBR2, have priorities 2 and 3 renumbering changes those priorities to 20 and 30. You can then add PBR3 with priority 25.

Synopsis

renumber ns pbrs

Example

renumber pbrs

apply ns pbrs

Updates the PBR's memory tree (lookup table), adding any new PBR and applying any modifications to existing PBRs. The lookup table includes the configuration of all the extended PBRs on the Citrix ADC. The Citrix ADC appliance uses the lookup table (not the configuration file) to filter the outgoing IPv4 packets.

Synopsis

apply ns pbrs

Arguments

Example

apply ns pbrs

ns-rateControl

The following operations can be performed on "ns-rateControl":

set| unset| show|

set ns rateControl

Sets the UDP/TCP/ICMP packet rate controls for any application that is not configured at System (direct access to the backend through System).

Synopsis

set ns rateControl

Arguments

tcpThreshold Number of SYNs permitted per 10 milliseconds. Minimum value: 0

udpThreshold Number of UDP packets permitted per 10 milliseconds. Minimum value: 0

icmpThreshold Number of ICMP packets permitted per 10 milliseconds. Default value: 100 Minimum value: 0

tcprstThreshold The number of TCP RST packets permitted per 10 milli second. zero means rate control is disabled and 0xffffffff means every thing is rate controlled Default value: 100 Minimum value: 0

Example

The following command will set the SYN rate to 100, icmp rate to 10 and the udp rate to unlimited.

```
set ns ratecontrol -tcpThreshold 100 -udpThreshold 0 -icmpThreshold 10



The 'show ns rate control' command can be used to view the current
settings of the rate controls.
```

> show ns ratecontrol UDP threshold: 0 per 10 ms TCP threshold: 0 per 10 ms ICMP threshold: 100 per 10 ms Done

unset ns rateControl

Use this command to remove ns rateControl settings.Refer to the set ns rateControl command for meanings of the arguments.

Synopsis

unset ns rateControl

show ns rateControl

Displays the values configured for rate control on the appliance.

Synopsis

show ns rateControl

Arguments

Output

tcpThreshold Number of SYNs permitted per 10 milliseconds.

udpThreshold Number of UDP packets permitted per 10 milliseconds.

icmpThreshold Number of ICMP packets permitted per 10 milliseconds.

tcprstThreshold The number of TCP RST packets permitted per 10 milli second. zero means rate control is disabled and 0xffffffff means every thing is rate controlled

statusInterval Status interval in milliseconds.

Example

By default, there is no rate control for TCP/UDP and for ICMP it will be 100. The output of the "show ns ratecontrol" command, with default setting,

> show ns ratecontrol UDP threshold: 0 per 10 ms TCP threshold: 0 per 10 ms ICMP threshold: 100 per 10 ms Done

ns-rollbackcmd

The following operations can be performed on "ns-rollbackcmd":

show ns rollbackcmd

Generates the command(s) that can be used to roll back the command(s) that are specified in an input file.

For example, if you want to roll back the creation of a load balancing virtual server named vserver_test, you must include the 'add lb vserver vserver_test ..' command in the input file. The output of this command is the 'rm lb vserver vserver_test' command.

Synopsis

show ns rollbackcmd

Arguments

fileName File that contains the commands for which the rollback commands must be generated. Specify the full path of the file name.

outtype Format in which the rollback commands must be generated.

Possible values: cli, xml

Example

show ns rollbackcmd -file <file_name>

ns-rpcNode

The following operations can be performed on "ns-rpcNode":

unset| show| set|

unset ns rpcNode

Use this command to remove ns rpcNode settings.Refer to the set ns rpcNode command for meanings of the arguments.

Synopsis

unset ns rpcNode <IPAddress>

show ns rpcNode

Display a list of nodes currently communicating by using Remote Procedure Calls (RPC).

Synopsis

show ns rpcNode

Arguments

IPAddress IP address of the node.

Output

password Password.

srcIP The src ip used in communiction with the peer System node.

secure State of the channel when talking to the node.

flags Flags related to this rpcNode

validateCert validate the server certificate for secure SSL connections

devno count stateflag

Example

Following example shows list of nodes communicating using RPC:

```
sh rpcnode
```

1. ```
   IPAddress:    10.101.4.84 Password:  ..8a7b474124957776b56cf03b28
   Srcip: 1.1.1.1
   ```

2. ```
   IPAddress:    10.101.4.87 Password:  ..ca2a035465d22c
   Srcip: 2.2.2.2
   ```

Done

set ns rpcNode

Sets the authentication attributes associated with peer system node. All system nodes use Remote Procedure Calls (RPC) to communicate.

Synopsis

set ns rpcNode <IPAddress> {-password } [-secure (YES | NO)]

Arguments

IPAddress IP address of the node. This has to be in the same subnet as the NSIP address.

password Password to be used in authentication with the peer system node.

srcIP Source IP address to be used to communicate with the peer system node. The default value is 0, which means that the appliance uses the NSIP address as the source IP address.

secure State of the channel when talking to the node.

Possible values: YES, NO Default value: YES

validateCert validate the server certificate for secure SSL connections

Possible values: YES, NO Default value: NO

Example

Example-1: Failover configuration In a failover configuration define peer NS as: add node 1 10.101.4.87 Set peer ha-unit's password as: set ns rpcnode 10.101.4.87 -password testpass -secure yes

System will now use the configured password to authenticate with its failover unit.

Example-2: GSLB configuration In a GSLB configuration define peer NS GSLB site as: add gslb site us_east_coast remote 206.123.3.4 Set peer GSLB-NS's password as: set ns rpcnode 206.123.3.4 -password testrun

System will now use the configured password to authenticate with east-coast GSLB site.

ns-runningConfig

The following operations can be performed on "ns-runningConfig":

show ns runningConfig

Displays all the configurations that have been executed on the appliance, including the configurations that have not yet been saved. Note: The unsaved configurations are lost when the appliance is rebooted or shut down.

Synopsis

show ns runningConfig

Arguments

withDefaults Include default values of parameters that have not been explicitly configured. If this argument is disabled, such parameters are not included.

Output

response running config data as text blob

Related Commands

- show ns.conf

ns-savedConfig

The following operations can be performed on "ns-savedConfig":

show ns savedConfig

Displays the saved configurations.

Synopsis

show ns savedConfig

Arguments

Output

textBlob Text of the last saved configuration.

Related Commands

- save config, show runningconfig

ns-serviceFunction

The following operations can be performed on "ns-serviceFunction":

rm| add| show| set|

rm ns serviceFunction

Removes specified service function.

Synopsis

rm ns serviceFunction <serviceFunctionName>

Arguments

serviceFunctionName Name of the service function to be created. Leading character must be a number or letter. Other characters allowed, after the first character, are @ _ - . (period) : (colon) # and space ( ).

Example

rm servicefunction tcpopt

add ns serviceFunction

Add a service function.

Synopsis

add ns serviceFunction <serviceFunctionName> -ingressVLAN <positive_integer>

Arguments

serviceFunctionName Name of the service function to be created. Leading character must be a number or letter. Other characters allowed, after the first character, are @ _ - . (period) : (colon) # and space ( ).

ingressVLAN VLAN ID on which the traffic from service function reaches Citrix ADC. Minimum value: 1 Maximum value: 4094

Example

add servicefunction tcpopt -ingressVLAN vlan1

show ns serviceFunction

displays specified service function.

Synopsis

show ns serviceFunction

Arguments

serviceFunctionName Name of the service function to be created. Leading character must be a number or letter. Other characters allowed, after the first character, are @ _ - . (period) : (colon) # and space ( ).

Output

ingressVLAN VLAN ID on which the traffic from service function reaches Citrix ADC.

stateflag the field for stateflags.

devno count

Example

show servicefunction tcpopt

set ns serviceFunction

Set operation on a service function.

Synopsis

set ns serviceFunction <serviceFunctionName>

Arguments

serviceFunctionName Name of the service function to be created. Leading character must be a number or letter. Other characters allowed, after the first character, are @ _ - . (period) : (colon) # and space ( ).

ingressVLAN VLAN ID on which the traffic from service function reaches Citrix ADC. Minimum value: 1 Maximum value: 4094

Example

set servicefunction tcpopt -ingressVLAN vlan2

ns-servicePath

The following operations can be performed on "ns-servicePath":

rm| show| add| bind| unbind|

rm ns servicePath

Removes a ServicePath.

Synopsis

rm ns servicePath <servicePathName>

Arguments

servicePathName Name for the Service path. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

Example

rm servicepath SP1

show ns servicePath

Displays ServicePath.

Synopsis

show ns servicePath

Arguments

servicePathName Name for the Service path. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

Output

serviceFunction List of service functions constituting the chain.

index The serviceindex of each servicefunction in path.

stateflag the field for stateflags.

devno count

Example

show servicepath SC1

add ns servicePath

Creates a Servicepath.

Synopsis

add ns servicePath <servicePathName>

Arguments

servicePathName Name for the Service path. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

Example

add servicepath SP1

bind ns servicePath

Bind service functions to path to define the path.

Synopsis

bind ns servicePath <servicePathName> -serviceFunction <string> -index <positive_integer>

Arguments

servicePathName Name for the Service path. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

serviceFunction Name of the service function to bind to path.

index Integer to specify the order, lower the number denotes further down in service chain. Minimum value: 1

Example

bind servicepath SP1 -servicefunction SF1 -index 255

unbind ns servicePath

unbind servicefunctions from servicepath.

Synopsis

unbind ns servicePath <servicePathName> -serviceFunction <string>

Arguments

servicePathName Name for the Service path. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

serviceFunction Name of the ServiceFunction to bind to ServicePath.

Example

unbind servicepath SP1 -servicefunction SF1

ns-simpleacl

The following operations can be performed on "ns-simpleacl":

stat| add| show| rm| flush| clear|

stat ns simpleacl

Displays statistics related to the simple ACL rules.

Synopsis

stat ns simpleacl

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

SimpleACL hits (SACLHits) Packets matching a SimpleACL.

SimpleACL misses (SACLMiss) Packets not matching any SimpleACL.

SimpleACLs count (SACLsCount) Number of SimpleACLs configured.

Allow SimpleACL hits (SACLAllow) Total packets that matched a SimpleACL with action ALLOW and got consumed by Citrix ADC.

Bridge SimpleACL hits (SACLBdg) Total packets that matched a SimpleACL with action BRIDGE and got bridged by Citrix ADC.

Deny SimpleACL hits (SACLDeny) Packets dropped because they match SimpleACL (Access Control List) with processing mode set to DENY.

Example

stat simpleacl

Related Commands

- stat ns partition

add ns simpleacl

Adds a simple ACL rule to the Citrix ADC. Simple ACL rules filter IPv4 packets on the basis of their source IP addresses and, optionally, the destination port and/or protocol. Any packet with the characteristics specified in the simple ACL rule is dropped.

Synopsis

add ns simpleacl <aclname> <aclaction> -srcIP <ip_addr>

Arguments

aclname Name for the simple ACL rule. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the simple ACL rule is created.

aclaction Drop incoming IPv4 packets that match the simple ACL rule.

Possible values: DENY

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

srcIP IP address to match against the source IP address of an incoming IPv4 packet.

destPort Port number to match against the destination port number of an incoming IPv4 packet.

DestPort is mandatory while setting Protocol. Omitting the port number and protocol creates an all-ports and all protocols simple ACL rule, which matches any port and any protocol. In that case, you cannot create another simple ACL rule specifying a specific port and the same source IPv4 address. Minimum value: 1 Maximum value: 65535

protocol Protocol to match against the protocol of an incoming IPv4 packet. You must set this parameter if you have set the Destination Port parameter.

Possible values: TCP, UDP

TTL Number of seconds, in multiples of four, after which the simple ACL rule expires. If you do not want the simple ACL rule to expire, do not specify a TTL value. Minimum value: 4 Maximum value: 2147483647

Example

add simpleacl rule1 DENY -srcIP 1.1.1.1 -destPort 80 -protocol TCP add simpleacl rule2 DENY -srcIP 2.2.2.2 -TTL 600

show ns simpleacl

Displays settings of all the simple ACL rules or of the specified simple ACL rule. To display settings of all the simple ACL rules, run the command without any parameters. To display settings of a particular simple ACL rule, specify the name of the simple ACL rule.

Synopsis

show ns simpleacl

Arguments

aclname Name of the simple ACL rule whose details you want the Citrix ADC to display.

Output

aclaction Drop incoming IPv4 packets that match the simple ACL rule.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

srcIP Source IP address.

stateflag SACL state flag.

destPort Destination Port.

protocol Protocol associated with the ACL rule.

TTL Time to expire this ACL rule(in seconds).

time Time when this acl is added.

hits Number of hits for this ACL rule.

devno count

Example

show simpleacl rule1 Name: rule1 Action: DENY srcIP = 10.102.1.150 Protocol = TCP DestPort = 110 Hits: 5 TTL: 200(seconds)

rm ns simpleacl

Removes a simple ACL rule from the Citrix ADC.

Synopsis

rm ns simpleacl <aclname> ...

Arguments

aclname Name of the simple ACL rule that you want to remove.

Example

rm ns simpleacl rule1

flush ns simpleacl

Terminates all established IPv4 connections that match any of the newly configured simple ACL rules.

Note: If you plan to create more than one simple ACL rule and flush existing connections that match any of them, you can minimize the affect on performance by first creating all of the simple ACL rules and then running flush only once.

Synopsis

flush ns simpleacl -estSessions

Arguments

estSessions

clear ns simpleacl

Removes all simple ACL rules from the Citrix ADC.

Synopsis

clear ns simpleacl

ns-simpleacl6

The following operations can be performed on "ns-simpleacl6":

flush| stat| show| add| clear| rm|

flush ns simpleacl6

Terminates all established IPv6 connections that match any of the newly configured simple ACL6 rules.

Note: If you plan to create more than one simple ACL6 rule and flush existing connections that match any of them, you can minimize the affect on performance by first creating all of the simple ACL6 rules and then running flush only once.

Synopsis

flush ns simpleacl6 -estSessions

Arguments

estSessions

stat ns simpleacl6

Displays statistics related to the simple ACL6 rules.

Synopsis

stat ns simpleacl6

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

SimpleACL6 hits (SACL6Hits) Packets matching a SimpleACL6.

SimpleACL6 misses (SACL6Miss) Packets not matching any SimpleACL6.

SimpleACLs6 count (SACL6sCount) Number of SimpleACL6s configured.

Allow SimpleACL6 hits (SACL6Allow) Total packets that matched a SimpleACL6 with action ALLOW and got consumed by Citrix ADC.

Bridge SimpleACL6 hits (SACL6Bdg) Total packets that matched a SimpleACL6 with action BRIDGE and got bridged by Citrix ADC.

Deny SimpleACL6 hits (SACL6Deny) Packets dropped because they match SimpleACL6 with processing mode set to DENY.

Example

stat simpleacl6

Related Commands

- stat ns partition

show ns simpleacl6

Displays settings of all the simple ACL6 rules or of the specified simple ACL6 rule. To display settings of all the simple ACL6 rules, run the command without any parameters. To display settings of a particular simple ACL6 rule, specify the name of the simple ACL6 rule.

Synopsis

show ns simpleacl6

Arguments

aclname Name of the simple ACL6 rule whose settings you want the Citrix ADC to display.

Output

aclaction Action associated with the SACL6 rule.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

srcIPv6 Source IP6 address.

stateflag SACL6 state flag.

destPort Destination Port.

protocol Protocol associated with the ACL rule.

TTL Time to expire this ACL rule(in seconds).

hits Number of hits for this SACL6 rule.

time Time when this acl is added.

devno count

Example

show simpleacl6 rule1 Name: rule1 Action: DENY Hits: 5 srcIP6 = 3ffe:100:100::1 Protocol = TCP DestPort = 110 TTL: 200(seconds)

add ns simpleacl6

Adds a simple ACL6 rule to the Citrix ADC. Simple ACL6 rules filter IPv6 packets on the basis of their source IP addresses and, optionally, the destination port and/or protocol. Any packet with the characteristics specified in the simple ACL6 rule is dropped.

Synopsis

add ns simpleacl6 <aclname> <aclaction> -srcIPv6 <ipv6_addr|null>

Arguments

aclname Name for the simple ACL6 rule. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the simple ACL6 rule is created.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

aclaction Drop incoming IPv6 packets that match the simple ACL6 rule.

Possible values: DENY

srcIPv6 IP address to match against the source IP address of an incoming IPv6 packet.

destPort Port number to match against the destination port number of an incoming IPv6 packet.

DestPort is mandatory while setting Protocol. Omitting the port number and protocol creates an all-ports and all protocol simple ACL6 rule, which matches any port and any protocol. In that case, you cannot create another simple ACL6 rule specifying a specific port and the same source IPv6 address. Minimum value: 1 Maximum value: 65535

protocol Protocol to match against the protocol of an incoming IPv6 packet. You must set this parameter if you set the Destination Port parameter.

Possible values: TCP, UDP

TTL Number of seconds, in multiples of four, after which the simple ACL6 rule expires. If you do not want the simple ACL6 rule to expire, do not specify a TTL value. Minimum value: 4 Maximum value: 2147483647

Example

add simpleacl6 rule1 DENY -srcIP6 fe80::2c0:95ff:fec5:d9b8 -destPort 80 -protocol TCP add simpleacl rule2 DENY -srcIP6 3ffe:100:100::1 -TTL 600

clear ns simpleacl6

Removes all simple ACL6 rules from the Citrix ADC.

Synopsis

clear ns simpleacl6

Example

clear ns simpleacl6

rm ns simpleacl6

Removes a simple ACL6 rule from the Citrix ADC.

Synopsis

rm ns simpleacl6 <aclname> ...

Arguments

aclname Name of the simple ACL6 rule that you want to remove.

Example

rm ns simpleacl6 rule1

ns-sourceroutecachetable

The following operations can be performed on "ns-sourceroutecachetable":

show| flush|

show ns sourceroutecachetable

Displays the current source route cache table.

Synopsis

show ns sourceroutecachetable

Arguments

Output

sourceIP Source ip of the connection.

sourceMAC source MAC address of an incoming IPv6 packet.

vlan ID of the VLAN.

interface ID of an interface.

devno count stateflag

flush ns sourceroutecachetable

Flushes the current Source route cache table.

Synopsis

flush ns sourceroutecachetable

ns-spParams

The following operations can be performed on "ns-spParams":

unset| set| show|

unset ns spParams

Use this command to remove ns spParams settings.Refer to the set ns spParams command for meanings of the arguments.

Synopsis

unset ns spParams

set ns spParams

Sets surge protection attributes on the appliance.

Synopsis

set ns spParams

Arguments

baseThreshold Maximum number of server connections that can be opened before surge protection is activated. Default value: 200 Maximum value: 32767

throttle Rate at which the system opens connections to the server.

Possible values: Aggressive, Normal, Relaxed Default value: Normal

Example

set ns spparams -baseThreshold 1000 -throttle aggressive set ns spparams -throttle relaxed

show ns spParams

Displays the surge protection configuration on the appliance. Surge protection parameters are set by using the 'set ns spParams' command.

Synopsis

show ns spParams

Arguments

Output

baseThreshold The base threshold. This is the maximum number of server connections that can be open before surge protection is activated.

throttle Rate at which the system opens connections to the server.

Table Table.

builtin Flag to determine if sp param is built-in or not

feature The feature to be checked while applying this config

Example

> show ns spparams Surge Protection parameters: BaseThreshold: 200 Throttle: Normal Done

ns-stats

The following operations can be performed on "ns-stats":

clear| show|

clear ns stats

Clearing stats

Synopsis

clear ns stats <cleanuplevel>

Arguments

cleanuplevel The level of stats to be cleared. 'global' option will clear global counters only, 'all' option will clear all device counters also along with global counters. For both the cases only 'ever incrementing counters' i.e. total counters will be cleared.

Possible values: global, all

show ns stats

show ns stats is an alias for stat ns

Synopsis

show ns stats - alias for 'stat ns'

ns-surgeQ

The following operations can be performed on "ns-surgeQ":

flush ns surgeQ

Flushes the connections that are waiting in SurgeQ. SurgeQ contains the client connections waiting for a server connection.

Synopsis

flush ns surgeQ [-name <string>]

Arguments

name Name of a virtual server, service or service group for which the SurgeQ must be flushed.

serverName Name of a service group member. This argument is needed when you want to flush the SurgeQ of a service group.

port port on which server is bound to the entity(Servicegroup).

Example

To flush the surgeQ system wide, use the command: flush ns SurgeQ. To flush the surgeQ specific to a vserver/service/svcgrp use the command: flush ns SurgeQ -name <name> To flush the surgeQ specific to a svcgrp member, use the command: flush ns surgeQ [-name <string>]

ns-tcpParam

The following operations can be performed on "ns-tcpParam":

show| set| unset|

show ns tcpParam

Displays the TCP parameters configured on the Citrix ADC.

Synopsis

show ns tcpParam

Arguments

Output

WS Enable or disable window scaling.

WSVal Factor used to calculate the new window size. This argument is needed only when the window scaling is enabled.

SACK Enable or disable Selective ACKnowledgement (SACK).

learnVsvrMSS Enable or disable maximum segment size (MSS) learning for virtual servers.

maxBurst Maximum number of TCP segments allowed in a burst.

initialCwnd Initial maximum upper limit on the number of TCP packets that can be outstanding on the TCP link to the server.

recvBuffSize TCP Receive buffer size

delayedAck Timeout for TCP delayed ACK, in milliseconds.

downStateRST Flag to switch on RST on down services.

nagle Enable or disable the Nagle algorithm on TCP connections.

limitedPersist Limit the number of persist (zero window) probes.

oooQSize Maximum size of out-of-order packets queue. A value of 0 means no limit.

ackOnPush Immediate ACK on PUSH packet

maxPktPerMss Maximum packets per MSS

pktPerRetx Maximum packets per retransmission

minRTO Minimum retransmission timeout, in milliseconds, specified in 10-millisecond increments (value must yield a whole number if divided by 10).

slowStartIncr TCP slowstart increment factor

maxDynServerProbes Maximum number of probes that Citrix ADC can send out in 10 milliseconds, to dynamically learn a service. Citrix ADC probes for the existence of the origin in case of wildcard virtual server or services.

synHoldFastGiveup Maximum threshold. After crossing this threshold number of outstanding probes for origin, the Citrix ADC reduces the number of connection retries for probe connections.

maxSynholdPerprobe Limit the number of client connections (SYN) waiting for status of single probe. Any new SYN packets will be dropped.

maxSynhold Limit the number of client connections (SYN) waiting for status of probe system wide. Any new SYN packets will be dropped.

mssLearnInterval Duration, in seconds, to sample the Maximum Segment Size (MSS) of the services. The Citrix ADC determines the best MSS to set for the virtual server based on this

sampling. The argument to enable maximum segment size (MSS) for virtual servers must be enabled.

mssLearnDelay Frequency, in seconds, at which the virtual servers learn the Maximum segment size (MSS) from the services. The argument to enable maximum segment size (MSS) for virtual servers must be enabled.

maxTimeWaitConn Maximum number of connections to hold in the TCP TIME_WAIT state on a packet engine. New connections entering TIME_WAIT state are proactively cleaned up.

KAprobeUpdateLastactivity Update last activity for KA probes

maxSynAckRetx When 'syncookie' is disabled in the TCP profile that is bound to the virtual server or service, and the number of TCP SYN+ACK retransmission by Citrix ADC for that virtual server or service crosses this threshold, the Citrix ADC responds by using the TCP SYN-Cookie mechanism.

synAttackDetection Detect TCP SYN packet flood and send an SNMP trap.

connFlushIfNoMem Flush an existing connection if no memory can be obtained for new connection.

HALF_CLOSED_AND_IDLE: Flush a connection that is closed by us but not by peer, or failing that, a connection that is past configured idle time. New connection fails if no such connection can be found.

FIFO: If no half-closed or idle connection can be found, flush the oldest non-management connection, even if it is active. New connection fails if the oldest few connections are management connections.

Note: If you enable this setting, you should also consider lowering the zombie timeout and half-close timeout, while setting the Citrix ADC timeout.

See Also: connFlushThres argument below.

connFlushThres Flush an existing connection (as configured through -connFlushIfNoMem FIFO) if the system has more than specified number of connections, and a new connection is to be established. Note: This value may be rounded down to be a whole multiple of the number of packet engines running.

mptcpConCloseOnPassiveSF Accept DATA_FIN/FAST_CLOSE on passive subflow

mptcpChecksum Use MPTCP DSS checksum

mptcpSFtimeout The timeout value in seconds for idle mptcp subflows. If this timeout is not set, idle subflows are cleared after cltTimeout of vserver

mptcpSFReplaceTimeout The minimum idle time value in seconds for idle mptcp subflows after which the sublow is replaced by new incoming subflow if maximum subflow limit is reached. The priority for replacement is given to those subflow without any transaction

mptcpMaxSF Maximum number of subflow connections supported in established state per mptcp connection.

mptcpMaxPendingSF Maximum number of subflow connections supported in pending join state per mptcp connection.

mptcpPendingJoinThreshold Maximum system level pending join connections allowed.

mptcpRTOsToSwitchSF Number of RTO's at subflow level, after which MPCTP should start using other subflow.

mptcpUseBackupOnDSS When enabled, if NS receives a DSS on a backup subflow, NS will start using that subflow to send data. And if disabled, NS will continue to transmit on current chosen subflow. In case there is some error on a subflow (like RTO's/RST etc.) then NS can choose a backup subflow irrespective of this tunable.

TcpMaxRetries Number of RTO's after which a connection should be freed.

mptcpImmediateSFCloseOnFIN Allow subflows to close immediately on FIN before the DATA_FIN exchange is completed at mptcp level.

mptcpCloseMptcpSessionOnLastSFClose Allow to send DATA FIN or FAST CLOSE on mptcp connection while sending FIN or RST on the last subflow.

mptcpSendSFResetOption Allow MPTCP subflows to send TCP RST Reason (MP_TCPRST) Option while sending TCP RST.

mptcpFastCloseOption Allow to select option ACK or RESET to force the closure of an MPTCP connection abruptly.

mptcpReliableAddAddr If enabled, Citrix ADC retransmits MPTCP ADD-ADDR option if echo response is not received within the timeout interval. The retransmission is attempted only once.

tcpFastOpenCookieTimeout Timeout in seconds after which a new TFO Key is computed for generating TFO Cookie. If zero, the same key is used always. If timeout is less than 120seconds, NS defaults to 120seconds timeout.

builtin Flag to determine if the tcp param is built-in or not

feature The feature to be checked while applying this config

autosyncookietimeout Timeout for the server to function in syncookie mode after the synattack. This is valid if TCP syncookie is disabled on the profile and server acts in non syncookie mode by default.

tcpFinTimeout The amount of time in seconds, after which a TCP connnection in the TCP TIME-WAIT state is flushed.

compactTcpOptionNoop If enabled, non-negotiated TCP options are removed from the received packet while proxying it. By default, non-negotiated TCP options would be replaced by NOPs in the proxied packets. This option is not applicable for Citrix ADC generated packets.

delinkClientServerOnRST If enabled, Delink client and server connection, when there is outstanding data to be sent to the other side.

set ns tcpParam

Sets the TCP parameters for the Citrix ADC.

Synopsis

set ns tcpParam

Arguments

WS Enable or disable window scaling.

Possible values: ENABLED, DISABLED Default value: ENABLED

WSVal Factor used to calculate the new window size. This argument is needed only when the window scaling is enabled. Default value: 8 Minimum value: 0 Maximum value: 14

SACK Enable or disable Selective ACKnowledgement (SACK).

Possible values: ENABLED, DISABLED Default value: ENABLED

learnVsvrMSS Enable or disable maximum segment size (MSS) learning for virtual servers.

Possible values: ENABLED, DISABLED Default value: DISABLED

maxBurst Maximum number of TCP segments allowed in a burst. Default value: 6 Minimum value: 1 Maximum value: 255

initialCwnd Initial maximum upper limit on the number of TCP packets that can be outstanding on the TCP link to the server. Default value: 10 Minimum value: 1 Maximum value: 44

delayedAck Timeout for TCP delayed ACK, in milliseconds. Default value: 100 Minimum value: 10 Maximum value: 300

downStateRST Flag to switch on RST on down services.

Possible values: ENABLED, DISABLED Default value: DISABLED

nagle Enable or disable the Nagle algorithm on TCP connections.

Possible values: ENABLED, DISABLED Default value: DISABLED

limitedPersist Limit the number of persist (zero window) probes.

Possible values: ENABLED, DISABLED Default value: ENABLED

oooQSize Maximum size of out-of-order packets queue. A value of 0 means no limit. Default value: 300 Minimum value: 0 Maximum value: 65535

ackOnPush Send immediate positive acknowledgement (ACK) on receipt of TCP packets with PUSH flag.

Possible values: ENABLED, DISABLED Default value: ENABLED

maxPktPerMss Maximum number of TCP packets allowed per maximum segment size (MSS). Minimum value: 0 Maximum value: 1460

pktPerRetx Maximum limit on the number of packets that should be retransmitted on receiving a partial ACK. Default value: 1 Minimum value: 1 Maximum value: 100

minRTO Minimum retransmission timeout, in milliseconds, specified in 10-millisecond increments (value must yield a whole number if divided by 10). Default value: 1000 Minimum value: 10 Maximum value: 64000

slowStartIncr Multiplier that determines the rate at which slow start increases the size of the TCP transmission window after each acknowledgement of successful transmission. Default value: 2 Minimum value: 1 Maximum value: 100

maxDynServerProbes Maximum number of probes that Citrix ADC can send out in 10 milliseconds, to dynamically learn a service. Citrix ADC probes for the existence of the origin in

case of wildcard virtual server or services. Default value: 7 Minimum value: 1 Maximum value: 65535

synHoldFastGiveup Maximum threshold. After crossing this threshold number of outstanding probes for origin, the Citrix ADC reduces the number of connection retries for probe connections. Default value: 1024 Minimum value: 256 Maximum value: 65535

maxSynholdPerprobe Limit the number of client connections (SYN) waiting for status of single probe. Any new SYN packets will be dropped. Default value: 128 Minimum value: 1 Maximum value: 255

maxSynhold Limit the number of client connections (SYN) waiting for status of probe system wide. Any new SYN packets will be dropped. Default value: 16384 Minimum value: 256 Maximum value: 65535

mssLearnInterval Duration, in seconds, to sample the Maximum Segment Size (MSS) of the services. The Citrix ADC determines the best MSS to set for the virtual server based on this sampling. The argument to enable maximum segment size (MSS) for virtual servers must be enabled. Default value: 180 Minimum value: 1 Maximum value: 1048576

mssLearnDelay Frequency, in seconds, at which the virtual servers learn the Maximum segment size (MSS) from the services. The argument to enable maximum segment size (MSS) for virtual servers must be enabled. Default value: 3600 Minimum value: 1 Maximum value: 1048576

maxTimeWaitConn Maximum number of connections to hold in the TCP TIME_WAIT state on a packet engine. New connections entering TIME_WAIT state are proactively cleaned up. Default value: 7000 Minimum value: 1

maxSynAckRetx When 'syncookie' is disabled in the TCP profile that is bound to the virtual server or service, and the number of TCP SYN+ACK retransmission by Citrix ADC for that virtual server or service crosses this threshold, the Citrix ADC responds by using the TCP SYN-Cookie mechanism. Default value: 100 Minimum value: 100 Maximum value: 1048576

synAttackDetection Detect TCP SYN packet flood and send an SNMP trap.

Possible values: ENABLED, DISABLED Default value: ENABLED

connFlushIfNoMem Flush an existing connection if no memory can be obtained for new connection.

HALF_CLOSED_AND_IDLE: Flush a connection that is closed by us but not by peer, or failing that, a connection that is past configured idle time. New connection fails if no such connection can be found.

FIFO: If no half-closed or idle connection can be found, flush the oldest non-management connection, even if it is active. New connection fails if the oldest few connections are management connections.

Note: If you enable this setting, you should also consider lowering the zombie timeout and half-close timeout, while setting the Citrix ADC timeout.

See Also: connFlushThres argument below.

Possible values: NONE , HALFCLOSED_AND_IDLE, FIFO Default value: NSA_CONNFLUSH_NONE

connFlushThres Flush an existing connection (as configured through -connFlushIfNoMem FIFO) if the system has more than specified number of connections, and a new connection is to be established. Note: This value may be rounded down to be a whole multiple of the number of packet engines running. Minimum value: 1

mptcpConCloseOnPassiveSF Accept DATA_FIN/FAST_CLOSE on passive subflow

Possible values: ENABLED, DISABLED Default value: ENABLED

mptcpChecksum Use MPTCP DSS checksum

Possible values: ENABLED, DISABLED Default value: ENABLED

mptcpSFtimeout The timeout value in seconds for idle mptcp subflows. If this timeout is not set, idle subflows are cleared after cltTimeout of vserver Default value: 0 Maximum value: 31536000

mptcpSFReplaceTimeout The minimum idle time value in seconds for idle mptcp subflows after which the sublow is replaced by new incoming subflow if maximum subflow limit is reached. The priority for replacement is given to those subflow without any transaction Default value: 10 Maximum value: 31536000

mptcpMaxSF Maximum number of subflow connections supported in established state per mptcp connection. Default value: 4 Minimum value: 2 Maximum value: 6

mptcpMaxPendingSF Maximum number of subflow connections supported in pending join state per mptcp connection. Default value: 4 Minimum value: 0 Maximum value: 4

mptcpPendingJoinThreshold Maximum system level pending join connections allowed. Default value: 0 Minimum value: 0 Maximum value: 4294967294

mptcpRTOsToSwitchSF Number of RTO's at subflow level, after which MPCTP should start using other subflow. Default value: 2 Minimum value: 1 Maximum value: 6

mptcpUseBackupOnDSS When enabled, if NS receives a DSS on a backup subflow, NS will start using that subflow to send data. And if disabled, NS will continue to transmit on current chosen subflow. In case there is some error on a subflow (like RTO's/RST etc.) then NS can choose a backup subflow irrespective of this tunable.

Possible values: ENABLED, DISABLED Default value: ENABLED

TcpMaxRetries Number of RTO's after which a connection should be freed. Default value: 7 Minimum value: 1 Maximum value: 7

mptcpImmediateSFCloseOnFIN Allow subflows to close immediately on FIN before the DATA_FIN exchange is completed at mptcp level.

Possible values: ENABLED, DISABLED Default value: DISABLED

mptcpCloseMptcpSessionOnLastSFClose Allow to send DATA FIN or FAST CLOSE on mptcp connection while sending FIN or RST on the last subflow.

Possible values: ENABLED, DISABLED Default value: DISABLED

mptcpSendSFResetOption Allow MPTCP subflows to send TCP RST Reason (MP_TCPRST) Option while sending TCP RST.

Possible values: ENABLED, DISABLED Default value: DISABLED

mptcpFastCloseOption Allow to select option ACK or RESET to force the closure of an MPTCP connection abruptly.

Possible values: ACK, RESET Default value: ACK

mptcpReliableAddAddr If enabled, Citrix ADC retransmits MPTCP ADD-ADDR option if echo response is not received within the timeout interval. The retransmission is attempted only once.

Possible values: ENABLED, DISABLED Default value: DISABLED

tcpFastOpenCookieTimeout Timeout in seconds after which a new TFO Key is computed for generating TFO Cookie. If zero, the same key is used always. If timeout is less than 120seconds, NS defaults to 120seconds timeout. Default value: 0 Minimum value: 0 Maximum value: 31536000

autosyncookietimeout Timeout for the server to function in syncookie mode after the synattack. This is valid if TCP syncookie is disabled on the profile and server acts in non syncookie mode by default. Default value: 30 Minimum value: 7 Maximum value: 65535

tcpFinTimeout The amount of time in seconds, after which a TCP connnection in the TCP TIME-WAIT state is flushed. Default value: 40 Minimum value: 10 Maximum value: 240

compactTcpOptionNoop If enabled, non-negotiated TCP options are removed from the received packet while proxying it. By default, non-negotiated TCP options would be replaced by NOPs in the proxied packets. This option is not applicable for Citrix ADC generated packets.

Possible values: ENABLED, DISABLED Default value: DISABLED

delinkClientServerOnRST If enabled, Delink client and server connection, when there is outstanding data to be sent to the other side.

Possible values: ENABLED, DISABLED Default value: DISABLED

unset ns tcpParam

Use this command to remove ns tcpParam settings.Refer to the set ns tcpParam command for meanings of the arguments.

Synopsis

unset ns tcpParam

ns-tcpProfile

The following operations can be performed on "ns-tcpProfile":

rm| unset| add| show| set|

rm ns tcpProfile

Removes a TCP profile from the appliance.

Synopsis

rm ns tcpProfile <name>

Arguments

name Name of the TCP profile to be removed.

Example

rm tcpprofile <profile name>

unset ns tcpProfile

Removes the attributes of the TCP profile. Attributes for which a default value is available revert to their default values. Refer to the 'set ns tcpProfile' command for a description of the parameters..Refer to the set ns tcpProfile command for meanings of the arguments.

Synopsis

unset ns tcpProfile <name>

add ns tcpProfile

Adds a TCP profile to the Citrix ADC.

Synopsis

add ns tcpProfile <name>

Arguments

name Name for a TCP profile. Must begin with a letter, number, or the underscore \(_\) character. Other characters allowed, after the first character, are the hyphen \(-\), period \(.\), hash \(#\), space \(\), at \(@\), colon \(:\), and equal \(=\) characters. The name of a TCP profile cannot be changed after it is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my tcp profile" or 'my tcp profile'\).

WS Enable or disable window scaling.

Possible values: ENABLED, DISABLED Default value: DISABLED

SACK Enable or disable Selective ACKnowledgement (SACK).

Possible values: ENABLED, DISABLED Default value: DISABLED

WSVal Factor used to calculate the new window size. This argument is needed only when window scaling is enabled. Default value: 4 Minimum value: 0 Maximum value: 14

nagle Enable or disable the Nagle algorithm on TCP connections.

Possible values: ENABLED, DISABLED Default value: DISABLED

ackOnPush Send immediate positive acknowledgement (ACK) on receipt of TCP packets with PUSH flag.

Possible values: ENABLED, DISABLED Default value: ENABLED

mss Maximum number of octets to allow in a TCP data segment. Minimum value: 0 Maximum value: 9176

maxBurst Maximum number of TCP segments allowed in a burst. Default value: 6 Minimum value: 1 Maximum value: 255

initialCwnd Initial maximum upper limit on the number of TCP packets that can be outstanding on the TCP link to the server. Default value: 4 Minimum value: 1 Maximum value: 44

delayedAck Timeout for TCP delayed ACK, in milliseconds. Default value: 100 Minimum value: 10 Maximum value: 300

oooQSize Maximum size of out-of-order packets queue. A value of 0 means no limit. Default value: 64 Minimum value: 0 Maximum value: 65535

maxPktPerMss Maximum number of TCP packets allowed per maximum segment size (MSS). Minimum value: 0 Maximum value: 1460

pktPerRetx Maximum limit on the number of packets that should be retransmitted on receiving a partial ACK. Default value: 1 Minimum value: 1 Maximum value: 512

minRTO Minimum retransmission timeout, in milliseconds, specified in 10-millisecond increments (value must yield a whole number if divided by 10). Default value: 1000 Minimum value: 10 Maximum value: 64000

slowStartIncr Multiplier that determines the rate at which slow start increases the size of the TCP transmission window after each acknowledgement of successful transmission. Default value: 2 Minimum value: 1 Maximum value: 100

bufferSize TCP buffering size, in bytes. Default value: 8190 Minimum value: 8190 Maximum value: 20971520

synCookie Enable or disable the SYNCOOKIE mechanism for TCP handshake with clients. Disabling SYNCOOKIE prevents SYN attack protection on the Citrix ADC.

Possible values: ENABLED, DISABLED Default value: ENABLED

KAprobeUpdateLastactivity Update last activity for the connection after receiving keep-alive (KA) probes.

Possible values: ENABLED, DISABLED Default value: ENABLED

flavor Set TCP congestion control algorithm.

Possible values: Default, Westwood, BIC, CUBIC, Nile Default value: Default

dynamicReceiveBuffering Enable or disable dynamic receive buffering. When enabled, allows the receive buffer to be adjusted dynamically based on memory and network conditions. Note: The buffer size argument must be set for dynamic adjustments to take place.

Possible values: ENABLED, DISABLED Default value: DISABLED

KA Send periodic TCP keep-alive (KA) probes to check if peer is still up.

Possible values: ENABLED, DISABLED Default value: DISABLED

KAconnIdleTime Duration, in seconds, for the connection to be idle, before sending a keep-alive (KA) probe. Default value: NSTCP_KA_DEFAULT_CONN_IDLETIME Minimum value: 1 Maximum value: 4095

KAmaxProbes Number of keep-alive (KA) probes to be sent when not acknowledged, before assuming the peer to be down. Default value: NSTCP_KA_DEFAULT_PROBE_COUNT Minimum value: 1 Maximum value: 254

KAprobeInterval Time interval, in seconds, before the next keep-alive (KA) probe, if the peer does not respond. Default value: NSTCP_KA_DEFAULT_INTERVAL Minimum value: 1 Maximum value: 4095

sendBuffsize TCP Send Buffer Size Default value: 8190 Minimum value: 8190 Maximum value: 20971520

mptcp Enable or disable Multipath TCP.

Possible values: ENABLED, DISABLED Default value: DISABLED

EstablishClientConn Establishing Client Client connection on First data/ Final-ACK / Automatic

Possible values: AUTOMATIC, CONN_ESTABLISHED, ON_FIRST_DATA Default value: AUTOMATIC

tcpSegOffload Offload TCP segmentation to the NIC. If set to AUTOMATIC, TCP segmentation will be offloaded to the NIC, if the NIC supports it.

Possible values: AUTOMATIC, DISABLED Default value: AUTOMATIC

rstWindowAttenuate Enable or disable RST window attenuation to protect against spoofing. When enabled, will reply with corrective ACK when a sequence number is invalid.

Possible values: ENABLED, DISABLED Default value: DISABLED

rstMaxAck Enable or disable acceptance of RST that is out of window yet echoes highest ACK sequence number. Useful only in proxy mode.

Possible values: ENABLED, DISABLED Default value: DISABLED

spoofSynDrop Enable or disable drop of invalid SYN packets to protect against spoofing. When disabled, established connections will be reset when a SYN packet is received.

Possible values: ENABLED, DISABLED Default value: ENABLED

ecn Enable or disable TCP Explicit Congestion Notification.

Possible values: ENABLED, DISABLED Default value: DISABLED

mptcpDropDataOnPreEstSF Enable or disable silently dropping the data on Pre-Established subflow. When enabled, DSS data packets are dropped silently instead of dropping the connection when data is received on pre established subflow.

Possible values: ENABLED, DISABLED Default value: DISABLED

mptcpFastOpen Enable or disable Multipath TCP fastopen. When enabled, DSS data packets are accepted before receiving the third ack of SYN handshake.

Possible values: ENABLED, DISABLED Default value: DISABLED

mptcpSessionTimeout MPTCP session timeout in seconds. If this value is not set, idle MPTCP sessions are flushed after vserver's client idle timeout. Default value: 0 Minimum value: 0 Maximum value: 86400

TimeStamp Enable or Disable TCP Timestamp option (RFC 1323)

Possible values: ENABLED, DISABLED Default value: DISABLED

dsack Enable or disable DSACK.

Possible values: ENABLED, DISABLED Default value: ENABLED

ackAggregation Enable or disable ACK Aggregation.

Possible values: ENABLED, DISABLED Default value: DISABLED

frto Enable or disable FRTO (Forward RTO-Recovery).

Possible values: ENABLED, DISABLED Default value: DISABLED

maxcwnd TCP Maximum Congestion Window. Default value: 524288 Minimum value: 8190 Maximum value: 20971520

fack Enable or disable FACK (Forward ACK).

Possible values: ENABLED, DISABLED Default value: DISABLED

tcpmode TCP Optimization modes TRANSPARENT / ENDPOINT.

Possible values: TRANSPARENT, ENDPOINT Default value: TRANSPARENT

tcpFastOpen Enable or disable TCP Fastopen. When enabled, NS can receive or send Data in SYN or SYN-ACK packets.

Possible values: ENABLED, DISABLED Default value: DISABLED

Hystart Enable or disable CUBIC Hystart

Possible values: ENABLED, DISABLED Default value: DISABLED

dupackthresh TCP dupack threshold. Default value: 3 Minimum value: 1 Maximum value: 15

burstRateControl TCP Burst Rate Control DISABLED/FIXED/DYNAMIC. FIXED requires a TCP rate to be set.

Possible values: DISABLED, FIXED, DYNAMIC Default value: DISABLED

tcprate TCP connection payload send rate in Kb/s Default value: 0 Minimum value: 0 Maximum value: 10000000

rateqmax Maximum connection queue size in bytes, when BurstRateControl is used Default value: 0 Minimum value: 0 Maximum value: 1000000000

DropHalfClosedConnOnTimeout Silently drop tcp half closed connections on idle timeout

Possible values: ENABLED, DISABLED Default value: DISABLED

DropEstConnOnTimeout Silently drop tcp established connections on idle timeout

Possible values: ENABLED, DISABLED Default value: DISABLED

applyAdaptiveTcp Apply Adaptive TCP optimizations

Possible values: ENABLED, DISABLED Default value: DISABLED

tcpFastOpenCookieSize TCP FastOpen Cookie size. This accepts only even numbers. Odd number is trimmed down to nearest even number. Default value: 8 Minimum value: 4 Maximum value: 16

taillossprobe TCP tail loss probe optimizations

Possible values: ENABLED, DISABLED Default value: DISABLED

clientIpTcpOption Client IP in TCP options

Possible values: ENABLED, DISABLED Default value: DISABLED

clientIpTcpOptionNumber ClientIP TCP Option number Minimum value: 1 Maximum value: 254

mpCapableCbit Set C bit in MP-CAPABLE Syn-Ack sent by Citrix ADC

Possible values: ENABLED, DISABLED Default value: DISABLED

sendClientPortInTcpOption Send Client Port number along with Client IP in TCP-Options. ClientIpTcpOption must be ENABLED

Possible values: ENABLED, DISABLED Default value: DISABLED

slowStartThreshold TCP Slow Start Threhsold Value. Default value: 524288 Minimum value: 8190 Maximum value: 20971520

Example

add tcpprofile <profile name> -WS ENABLED -WSVAL 4

show ns tcpProfile

Displays information about TCP profiles configured on the appliance.

Synopsis

show ns tcpProfile

Arguments

name Name of the TCP profile to be displayed. If a name is not provided, information about all TCP profiles is shown.

Output

WS Enable or disable window scaling.

SACK Enable or disable Selective ACKnowledgement (SACK).

WSVal Factor used to calculate the new window size. This argument is needed only when window scaling is enabled.

nagle Enable or disable the Nagle algorithm on TCP connections.

ackOnPush Send immediate positive acknowledgement (ACK) on receipt of TCP packets with PUSH flag.

mss Maximum Segment Size(MSS) to use for TCP Connection(0 forces use of global setting)

maxBurst Maximum number of TCP segments allowed in a burst.

initialCwnd Initial maximum upper limit on the number of TCP packets that can be outstanding on the TCP link to the server.

delayedAck Timeout for TCP delayed ACK, in milliseconds.

oooQSize Maximum size of out-of-order packets queue. A value of 0 means no limit.

maxPktPerMss Maximum packet per MSS value

pktPerRetx Maximum limit on the number of packets that should be retransmitted on receiving a partial ACK.

minRTO TCP minimum RTO (in millisec)

slowStartIncr TCP slowstart increment factor

bufferSize TCP Buffer size

flavor TCP algorithm

refCnt Number of entities using this profile

synCookie Enable or disable the SYNCOOKIE mechanism for TCP handshake with clients. Disabling SYNCOOKIE prevents SYN attack protection on the Citrix ADC.

KAprobeUpdateLastactivity Update last activity for the connection after receiving keep-alive (KA) probes.

dynamicReceiveBuffering Enable or disable dynamic receive buffering. When enabled, allows the receive buffer to be adjusted dynamically based on memory and network conditions. Note: The buffer size argument must be set for dynamic adjustments to take place.

KA Send periodic TCP keep-alive (KA) probes to check if peer is still up.

KAconnIdleTime Duration, in seconds, for the connection to be idle, before sending a keep-alive (KA) probe.

KAmaxProbes Number of keep-alive (KA) probes to be sent when not acknowledged, before assuming the peer to be down.

KAprobeInterval Time interval, in seconds, before the next keep-alive (KA) probe, if the peer does not respond.

sendBuffsize TCP Send Buffer size

mptcp Enable/Disable Multi-Path TCP

EstablishClientConn Allocating Client Conn on

tcpSegOffload TCP Segmentation Offload

rstWindowAttenuate RST Window Attenuation

rstMaxAck accept RST with max ACK

TimeStamp TCP Timestamp Option

spoofSynDrop drop invalid SYN packets

ecn Explicit Congestion Notification

mptcpDropDataOnPreEstSF Enable or disable dropping data on pre established subflow.

mptcpFastOpen Enable or disable MPTCP fastopen.

mptcpSessionTimeout MPTCP session timeout.

dsack Enable or disable DSACK.

ackAggregation Enable or disable ACK Aggregation.

frto Enable or disable FRTO (Forward RTO-Recovery).

maxcwnd TCP Maximum Congestion Window.

fack Forward Acknowlegement

tcpmode TCP Optimization mode

tcpFastOpen Enable or disable TCP fastopen.

Hystart TCP CUBIC Hystart

dupackthresh TCP Dupack Threshold

nileD1Percent TCP Nile D1 percent

nileD2Percent TCP Nile D2 percent

nileD3Percent TCP Nile D3 percent

nileBetaMaxPercent TCP Nile Beta max

nileBetaMinPercent TCP Nile Beta min

nileAlphaMax TCP Nile Alpha max

nileAlphaMinPercent TCP Nile Alpha min

nileRttFilter TCP Nile RTT filter

nileRttFactor TCP Nile RTT factor

burstRateControl TCP Burst Rate Control DISABLED/FIXED/DYNAMIC. FIXED requires a TCP rate to be set.

tcprate TCP connection payload send rate in Kb/s

rateqmax Maximum connection queue size in bytes, when BurstRateControl is used

DropHalfClosedConnOnTimeout Silently drop tcp half closed connections on idle timeout

DropEstConnOnTimeout Silently drop tcp established connections on idle timeout

stateflag State flag

isAdaptiveTcp Explicit Adaptive TCP profile

applyAdaptiveTcp Use Adaptive TCP optimizations

builtin Flag to determine if tcp profile is built-in or not

feature The feature to be checked while applying this config

tcpFastOpenCookieSize TCP FastOpen Cookie size. This accepts only even numbers. Odd number is trimmed down to nearest even number.

taillossprobe TCP tail loss probe optimizations

clientIpTcpOption Client IP in TCP options

clientIpTcpOptionNumber ClientIP TCP Option number

mpCapableCbit Set C bit in MP-CAPABLE Syn-Ack sent by Citrix ADC

sendClientPortInTcpOption Send Client Port along with Client IP in TCP option

slowStartThreshold Slow Start Threshold Value

devno count

Example

show tcp profile

set ns tcpProfile

Modifies the attributes of a TCP profile.

Synopsis

set ns tcpProfile <name>

Arguments

name Name of the TCP profile to be modified.

WS Enable or disable window scaling.

Possible values: ENABLED, DISABLED Default value: DISABLED

SACK Enable or disable Selective ACKnowledgement (SACK).

Possible values: ENABLED, DISABLED Default value: DISABLED

WSVal Factor used to calculate the new window size. This argument is needed only when window scaling is enabled. Default value: 4 Minimum value: 0 Maximum value: 14

nagle Enable or disable the Nagle algorithm on TCP connections.

Possible values: ENABLED, DISABLED Default value: DISABLED

ackOnPush Send immediate positive acknowledgement (ACK) on receipt of TCP packets with PUSH flag.

Possible values: ENABLED, DISABLED Default value: ENABLED

mss Set Maximum Segment Size(MSS) to use for TCP Connection(0 forces use of global setting) Minimum value: 0 Maximum value: 9176

maxBurst Maximum number of TCP segments allowed in a burst. Default value: 6 Minimum value: 1 Maximum value: 255

initialCwnd Initial maximum upper limit on the number of TCP packets that can be outstanding on the TCP link to the server. Default value: 4 Minimum value: 1 Maximum value: 44

delayedAck Timeout for TCP delayed ACK, in milliseconds. Default value: 100 Minimum value: 10 Maximum value: 300

oooQSize Maximum size of out-of-order packets queue. A value of 0 means no limit. Default value: 64 Minimum value: 0 Maximum value: 65535

maxPktPerMss Maximum number of TCP packets allowed per maximum segment size (MSS). Minimum value: 0 Maximum value: 1460

pktPerRetx Maximum limit on the number of packets that should be retransmitted on receiving a partial ACK. Default value: 1 Minimum value: 1 Maximum value: 512

minRTO Minimum retransmission timeout, in milliseconds, specified in 10-millisecond increments (value must yield a whole number if divided by 10). Default value: 1000 Minimum value: 10 Maximum value: 64000

slowStartIncr Multiplier that determines the rate at which slow start increases the size of the TCP transmission window after each acknowledgement of successful transmission. Default value: 2 Minimum value: 1 Maximum value: 100

bufferSize TCP buffering size, in bytes. Default value: 8190 Minimum value: 8190 Maximum value: 20971520

synCookie Enable or disable the SYNCOOKIE mechanism for TCP handshake with clients. Disabling SYNCOOKIE prevents SYN attack protection on the Citrix ADC.

Possible values: ENABLED, DISABLED Default value: ENABLED

KAprobeUpdateLastactivity Update last activity for the connection after receiving keep-alive (KA) probes.

Possible values: ENABLED, DISABLED Default value: ENABLED

flavor Set TCP congestion control algorithm.

Possible values: Default, Westwood, BIC, CUBIC, Nile Default value: Default

dynamicReceiveBuffering Enable or disable dynamic receive buffering. When enabled, allows the receive buffer to be adjusted dynamically based on memory and network conditions. Note: The buffer size argument must be set for dynamic adjustments to take place.

Possible values: ENABLED, DISABLED Default value: DISABLED

KA Send periodic TCP keep-alive (KA) probes to check if peer is still up.

Possible values: ENABLED, DISABLED Default value: DISABLED

KAconnIdleTime Duration, in seconds, for the connection to be idle, before sending a keep-alive (KA) probe. Default value: NSTCP_KA_DEFAULT_CONN_IDLETIME Minimum value: 1 Maximum value: 4095

KAmaxProbes Number of keep-alive (KA) probes to be sent when not acknowledged, before assuming the peer to be down. Default value: NSTCP_KA_DEFAULT_PROBE_COUNT Minimum value: 1 Maximum value: 254

KAprobeInterval Time interval, in seconds, before the next keep-alive (KA) probe, if the peer does not respond. Default value: NSTCP_KA_DEFAULT_INTERVAL Minimum value: 1 Maximum value: 4095

sendBuffsize TCP Send Buffer Size Default value: 8190 Minimum value: 8190 Maximum value: 20971520

mptcp Enable or disable Multipath TCP.

Possible values: ENABLED, DISABLED Default value: DISABLED

EstablishClientConn Establishing Client Client connection on First data/ Final-ACK / Automatic

Possible values: AUTOMATIC, CONN_ESTABLISHED, ON_FIRST_DATA Default value: AUTOMATIC

tcpSegOffload Offload TCP segmentation to the NIC. If set to AUTOMATIC, TCP segmentation will be offloaded to the NIC, if the NIC supports it.

Possible values: AUTOMATIC, DISABLED Default value: AUTOMATIC

rstWindowAttenuate Enable or disable RST window attenuation to protect against spoofing. When enabled, will reply with corrective ACK when a sequence number is invalid.

Possible values: ENABLED, DISABLED Default value: DISABLED

rstMaxAck Enable or disable acceptance of RST that is out of window yet echoes highest ACK sequence number. Useful only in proxy mode.

Possible values: ENABLED, DISABLED Default value: DISABLED

spoofSynDrop Enable or disable drop of invalid SYN packets to protect against spoofing. When disabled, established connections will be reset when a SYN packet is received.

Possible values: ENABLED, DISABLED Default value: ENABLED

ecn Enable or disable TCP Explicit Congestion Notification.

Possible values: ENABLED, DISABLED Default value: DISABLED

mptcpDropDataOnPreEstSF Enable or disable silently dropping the data on Pre-Established subflow. When enabled, DSS data packets are dropped silently instead of dropping the connection when data is received on pre established subflow.

Possible values: ENABLED, DISABLED Default value: DISABLED

mptcpFastOpen Enable or disable Multipath TCP fastopen. When enabled, DSS data packets are accepted before receiving the third ack of SYN handshake.

Possible values: ENABLED, DISABLED Default value: DISABLED

mptcpSessionTimeout MPTCP session timeout in seconds. If this value is not set, idle MPTCP sessions are flushed after vserver's client idle timeout. Default value: 0 Minimum value: 0 Maximum value: 86400

TimeStamp Enable or Disable TCP Timestamp option (RFC 1323)

Possible values: ENABLED, DISABLED Default value: DISABLED

dsack Enable or disable DSACK.

Possible values: ENABLED, DISABLED Default value: ENABLED

ackAggregation Enable or disable ACK Aggregation.

Possible values: ENABLED, DISABLED Default value: DISABLED

frto Enable or disable FRTO (Forward RTO-Recovery).

Possible values: ENABLED, DISABLED Default value: DISABLED

maxcwnd TCP Maximum Congestion Window. Default value: 524288 Minimum value: 8190 Maximum value: 20971520

fack Enable or disable FACK (Forward ACK).

Possible values: ENABLED, DISABLED Default value: DISABLED

tcpmode TCP Optimization modes TRANSPARENT / ENDPOINT.

Possible values: TRANSPARENT, ENDPOINT Default value: TRANSPARENT

tcpFastOpen Enable or disable TCP Fastopen. When enabled, NS can receive or send Data in SYN or SYN-ACK packets.

Possible values: ENABLED, DISABLED Default value: DISABLED

Hystart Enable or disable CUBIC Hystart

Possible values: ENABLED, DISABLED Default value: DISABLED

dupackthresh TCP dupack threshold. Default value: 3 Minimum value: 1 Maximum value: 15

burstRateControl TCP Burst Rate Control DISABLED/FIXED/DYNAMIC. FIXED requires a TCP rate to be set.

Possible values: DISABLED, FIXED, DYNAMIC Default value: DISABLED

tcprate TCP connection payload send rate in Kb/s Default value: 0 Minimum value: 0 Maximum value: 10000000

rateqmax Maximum connection queue size in bytes, when BurstRateControl is used Default value: 0 Minimum value: 0 Maximum value: 1000000000

DropHalfClosedConnOnTimeout Silently drop tcp half closed connections on idle timeout

Possible values: ENABLED, DISABLED Default value: DISABLED

DropEstConnOnTimeout Silently drop tcp established connections on idle timeout

Possible values: ENABLED, DISABLED Default value: DISABLED

applyAdaptiveTcp Apply Adaptive TCP optimizations

Possible values: ENABLED, DISABLED Default value: DISABLED

tcpFastOpenCookieSize TCP FastOpen Cookie size. This accepts only even numbers. Odd number is trimmed down to nearest even number. Default value: 8 Minimum value: 4 Maximum value: 16

taillossprobe TCP tail loss probe optimizations

Possible values: ENABLED, DISABLED Default value: DISABLED

clientIpTcpOption Client IP in TCP options

Possible values: ENABLED, DISABLED Default value: DISABLED

clientIpTcpOptionNumber ClientIP TCP Option number Minimum value: 1 Maximum value: 254

mpCapableCbit Set C bit in MP-CAPABLE Syn-Ack sent by Citrix ADC

Possible values: ENABLED, DISABLED Default value: DISABLED

sendClientPortInTcpOption Send Client Port number along with Client IP in TCP-Options. ClientIpTcpOption must be ENABLED

Possible values: ENABLED, DISABLED Default value: DISABLED

slowStartThreshold TCP Slow Start Threhsold Value. Default value: 524288 Minimum value: 8190 Maximum value: 20971520

Example

set tcpprofile <profile name> -WS ENABLED -WSVAL 4

ns-tcpbufParam

The following operations can be performed on "ns-tcpbufParam":

show| set| unset|

show ns tcpbufParam

Displays the TCP buffering configuration on the appliance.

Synopsis

show ns tcpbufParam

Arguments

Output

size TCP buffering size per connection, in kilobytes.

memLimit Maximum memory, in megabytes, that can be used for buffering.

builtin Flag to determine if TCP buffering is built-in or not

feature The feature to be checked while applying this config

Example

An example of this command's output is as follows: TCP buffer size: 64KBytes TCP buffer percentage: 50%

set ns tcpbufParam

Sets the attributes for the TCP buffering per connection.

Synopsis

set ns tcpbufParam

Arguments

size TCP buffering size per connection, in kilobytes. Default value: 64 Minimum value: 4 Maximum value: 20480

memLimit Maximum memory, in megabytes, that can be used for buffering. Default value: 64

unset ns tcpbufParam

Use this command to remove ns tcpbufParam settings.Refer to the set ns tcpbufParam command for meanings of the arguments.

Synopsis

unset ns tcpbufParam

ns-testlicense

The following operations can be performed on "ns-testlicense":

show| apply|

show ns testlicense

Displays the state of test license features. Usage:

1. Copy the license file(s) which are to be tested in "/nsconfig/testlicense".
2. Run "show ns testlicense" to display all available features and expiration days.

Same is available through GUI at "System -> Licences -> ADC Test License"

Synopsis

show ns testlicense

Arguments

Output

WL Web Logging.

SP Surge Protection.

LB Load Balancing.

CS Content Switching.

CR Cache Redirect.

CMP Compression.

DELTA Delta Compression.

SSL Secure Sockets Layer.

GSLB Global Server Load Balancing.

GSLBP GSLB Proximity.

Routing Routing.

CF Content Filter.

ContentAccelerator transparent Integrated Caching.

IC Integrated Caching.

SSLVPN SSL VPN.

AAA AAA

OSPF OSPF Routing.

RIP RIP Routing.

BGP BGP Routing.

REWRITE Rewrite.

IPv6PT IPv6 protocol translation

AppFw Application Firewall.

RESPONDER Responder.

AGEE NSXN ModelID Model Number ID. Represents different numbers for two types of licenses.:

- Bandwidth licenses - specifies the throughput bandwidth licensed for this appliance e.g. (For 20 Gbps) Model Number ID: 20000
- vCPU licenses - specifies number of vCPUs licensed for this appliance. e.g. (For 4 vCPU) Model Number ID: 4 vCPUs

push Citrix ADC Push.

AppFlow AppFlow.

CloudBridge CloudBridge.

CloudBridgeAppliance CloudExtenderAppliance ISIS ISIS Routing.

Cluster Clustering

CH Call Home.

AppQoE AppQoS

APPFLOWICA Appflow for ICA

isStandardLic Standard License

isEnterpriseLic Enterprise License

isPlatinumLic Platinum License

isSGwyLic Simple Gateway License

isSWGLic Secure Web Gateway License

DiskCaching Integrated Disk Cache

FEO Front End Optimization

LSN Large Scale NAT.

licensingMode Pooled Licensed.

daysToExpiration Days to expire.

RDPProxy RDPPROXY.

Rep Reputation Services.

URLFiltering URL Filtering.

VideoOptimization Video Optimization.

ForwardProxy Forward Proxy.

SSLInterception SSL Interception.

RemoteContentInspection Remote Content Inspection.

AdaptiveTCP Adaptive TCP.

CQA Connection Quality Analytics.

Bot Bot Management.

APIGateway API Gateway

apply ns testlicense

Apply test license Use this command to apply license(s) tested using "show ns testlicense" command.

Synopsis

apply ns testlicense

Example

apply ns testlicense

ns-timeout

The following operations can be performed on "ns-timeout":

unset| show| set|

unset ns timeout

Use this command to remove ns timeout settings.Refer to the set ns timeout command for meanings of the arguments.

Synopsis

unset ns timeout

show ns timeout

Displays the timeouts configured for various Citrix ADC entities. Note: The timeouts having default values are not displayed.

Synopsis

show ns timeout

Arguments

Output

zombie Timer interval(in seconds) for zombie process that cleanup inactive TCP connections Minimum value: 1 Maximum value: 600 Default value: 120

client Client idle timeout (in seconds). If zero, the service-type default value is taken when service is created.

server Server idle timeout (in seconds). If zero, the service-type default value is taken when service is created.

httpClient HTTP client idle timeout (in seconds) Minimum value: 0 Maximum value: 18000

httpServer HTTP server idle timeout (in seconds) Minimum value: 0 Maximum value: 18000

tcpClient TCP client idle timeout (in seconds) Minimum value: 0 Maximum value: 18000

tcpServer TCP server idle timeout (in seconds) Minimum value: 0 Maximum value: 18000

anyClient ANY client idle timeout (in seconds) Minimum value: 0 Maximum value: 31536000

anyServer ANY server idle timeout (in seconds) Minimum value: 0 Maximum value: 31536000

halfclose Half-closed connection timeout (in seconds) Minimum value: 1 Maximum value: 600 Default value: 10

anyTcpClient Global idle timeout, in seconds, for TCP client connections. This value takes precedence over entity level timeout settings (vserver/service). This is applicable only to transport protocol TCP.

anyTcpServer Global idle timeout, in seconds, for TCP server connections. This value takes precedence over entity level timeout settings (vserver/service). This is applicable only to transport protocol TCP.

nontcpZombie Timer interval(in seconds) for zombie process that cleanup inactive IP NAT connections Minimum value: 1 Maximum value: 600 Default value: 60

ReducedFinTimeOut Timer interval(in seconds) for NATPCB for tcp flow

ReducedRstTimeOut Timer interval(in seconds) for NATPCB for tcp flow

NewConnIdleTimeOut Timer interval(in seconds) for new NATPCB for tcp connections

Example

show ns timeout

set ns timeout

Sets timeout values for various aspects of the Citrix ADC. Caution: Modifying these values can affect system performance.

Synopsis

set ns timeout

Arguments

zombie Interval, in seconds, at which the Citrix ADC zombie cleanup process must run. This process cleans up inactive TCP connections. Default value: 120 Minimum value: 1 Maximum value: 600

httpClient Global idle timeout, in seconds, for client connections of HTTP service type. This value is over ridden by the client timeout that is configured on individual entities. Default value: 0 Minimum value: 0 Maximum value: 18000

httpServer Global idle timeout, in seconds, for server connections of HTTP service type. This value is over ridden by the server timeout that is configured on individual entities. Default value: 0 Minimum value: 0 Maximum value: 18000

tcpClient Global idle timeout, in seconds, for non-HTTP client connections of TCP service type. This value is over ridden by the client timeout that is configured on individual entities. Default value: 0 Minimum value: 0 Maximum value: 18000

tcpServer Global idle timeout, in seconds, for non-HTTP server connections of TCP service type. This value is over ridden by the server timeout that is configured on entities. Default value: 0 Minimum value: 0 Maximum value: 18000

anyClient Global idle timeout, in seconds, for non-TCP client connections. This value is over ridden by the client timeout that is configured on individual entities. Default value: 0 Minimum value: 0 Maximum value: 31536000

anyServer Global idle timeout, in seconds, for non TCP server connections. This value is over ridden by the server timeout that is configured on individual entities. Default value: 0 Minimum value: 0 Maximum value: 31536000

anyTcpClient Global idle timeout, in seconds, for TCP client connections. This value takes precedence over entity level timeout settings (vserver/service). This is applicable only to transport protocol TCP. Default value: 0 Minimum value: 0 Maximum value: 31536000

anyTcpServer Global idle timeout, in seconds, for TCP server connections. This value takes precedence over entity level timeout settings (vserver/service). This is applicable only to transport protocol TCP. Default value: 0 Minimum value: 0 Maximum value: 31536000

halfclose Idle timeout, in seconds, for connections that are in TCP half-closed state. Default value: 10 Minimum value: 1 Maximum value: 600

nontcpZombie Interval at which the zombie clean-up process for non-TCP connections should run. Inactive IP NAT connections will be cleaned up. Default value: 60 Minimum value: 1 Maximum value: 600

ReducedFinTimeOut Alternative idle timeout, in seconds, for closed TCP NATPCB connections. Default value: 30 Minimum value: 1 Maximum value: 300

ReducedRstTimeOut Timer interval, in seconds, for abruptly terminated TCP NATPCB connections. Default value: 0 Minimum value: 0 Maximum value: 300

NewConnIdleTimeOut Timer interval, in seconds, for new TCP NATPCB connections on which no data was received. Default value: 4 Minimum value: 1 Maximum value: 120

Example

set ns timeout -zombie 200

ns-timer

The following operations can be performed on "ns-timer":

bind| unset| show| set| rm| rename| add| unbind|

bind ns timer

Defines the binding relation among timer, and timer policy.

Synopsis

bind ns timer <name> -policyName <string> -priority <positive_integer>

Arguments

name Timer name.

policyName The timer policy associated with the timer.

priority Priority with which the policy is to be bound. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE. o If gotoPriorityExpression is not present or if it is equal to END then the policy bank evaluation ends here o Else if the gotoPriorityExpression is equal to NEXT then the next policy in the priority order is evaluated. o Else gotoPriorityExpression is evaluated. The result of gotoPriorityExpression (which has to be a number) is processed as follows:

- An UNDEF event is triggered if . gotoPriorityExpression cannot be evaluated . gotoPriorityExpression evaluates to number which is smaller than the maximum priority in the policy bank but is not same as any policy's priority . gotoPriorityExpression evaluates to a priority that is smaller than the current policy's priority
- If the gotoPriorityExpression evaluates to the priority of the current policy then the next policy in the priority order is evaluated.
- If the gotoPriorityExpression evaluates to the priority of a policy further ahead in the list then that policy will be evaluated next.

vServer Name of the vserver which provides the context for the rule in timer policy. When not specified it is treated as a Global Default context.

sampleSize Denotes the sample size. Sample size value of 'x' means that previous '(x - 1)' policy's rule evaluation results and the current evaluation result are present with the binding. For example, sample size of 10 means that there is a state of previous 9 policy evaluation results and also the current policy evaluation result. Default value: 3 Minimum value: 1 Maximum value: 32

threshold Denotes the threshold. If the rule of the policy in the binding relation evaluates 'threshold size' number of times in 'sample size' to true, then the corresponding action is taken. Its value needs to be less than or equal to the sample size value. Default value: 3 Minimum value: 1 Maximum value: 32

Example

i) bind ns timer timer_trigger -policyName timer_pol -priority 1 ii) bind ns timer timer_trigger -policyName timer_pol -priority 1

unset ns timer

Unset comment for existing timer..Refer to the set ns timer command for meanings of the arguments.

Synopsis

unset ns timer <name>

Example

unset ns timer timer -comment

show ns timer

Display the Timer entities.

Synopsis

show ns timer

Arguments

name Timer name.

Output

interval The frequency at which the policies bound to this timer are invoked. The minimum value is 20 msec. The maximum value is 20940 in seconds and 349 in minutes

unit Timer interval unit

comment Comments associated with this timer.

policyName The timer policy associated with the timer.

priority Specifies the priority of the timer policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

vServer Name of the vserver which provides the context for the rule in timer policy. When not specified it is treated as a Global Default context.

sampleSize Denotes the sample size. Sample size value of 'x' means that previous '(x - 1)' policy's rule evaluation results and the current evaluation result are present with the binding. For example, sample size of 10 means that there is a state of previous 9 policy evaluation results and also the current policy evaluation result.

threshold Denotes the threshold. If the rule of the policy in the binding relation evaluates 'threshold size' number of times in 'sample size' to true, then the corresponding action is taken. Its value needs to be less than or equal to the sample size value.

stateflag bindPolicyType devno count

set ns timer

Set a argument values for existing timer.

Synopsis

set ns timer <name>

Arguments

name Timer name.

interval The frequency at which the policies bound to this timer are invoked. The minimum value is 20 msec. The maximum value is 20940 in seconds and 349 in minutes Default value: 5 Minimum value: 1 Maximum value: 20940000

unit Timer interval unit

Possible values: SEC, MIN Default value: SEC

comment Comments associated with this timer.

Example

set ns timer timer -comment "Timer that would be invoked at interval 20 sec apart."

rm ns timer

Remove a Timer.

Synopsis

rm ns timer <name>

Arguments

name Timer name.

Example

rm ns timer timer

rename ns timer

Rename a timer.

Synopsis

rename ns timer <name>@ <newName>@

Arguments

name The name of the timer.

newName The new name of the timer.

Example

rename ns timer oldname newname

add ns timer

Create a Timer.

Synopsis

add ns timer <name> (-interval <integer>)

Arguments

name Timer name.

interval The frequency at which the policies bound to this timer are invoked. The minimum value is 20 msec. The maximum value is 20940 in seconds and 349 in minutes Default value: 5 Minimum value: 1 Maximum value: 20940000

unit Timer interval unit

Possible values: SEC, MIN Default value: SEC

comment Comments associated with this timer.

Example

add timer policy timer -comment "Timer that would be invoked at interval 10 sec apart."

unbind ns timer

Unbind entities from timer

Synopsis

unbind ns timer <name> -policyName <string>

Arguments

name Timer name.

policyName The timer policy associated with the timer.

Example

unbind ns timer timer -policyName timer_pol

ns-timezone

The following operations can be performed on "ns-timezone":

show ns timezone

get all the available timezone option

Synopsis

show ns timezone

Arguments

value

Output

devno count stateflag

ns-trafficDomain

The following operations can be performed on "ns-trafficDomain":

disable| rm| unbind| bind| enable| stat| add| show| clear|

disable ns trafficDomain

Disable TrafficDomain. NOTE: This command is deprecated.Traffic domains related configuration commands are being deprecated and will be removed in a future release. Citrix recommends you to use admin partitions instead of using traffic domains

Synopsis

Arguments

td Integer value that uniquely identifies a traffic domain. Minimum value: 1 Maximum value: 4094

Example

disable ns trafficdomain 1

rm ns trafficDomain

Remove Traffic Domain configured. NOTE: This command is deprecated.Traffic domains related configuration commands are being deprecated and will be removed in a future release. Citrix recommends you to use admin partitions instead of using traffic domains

Synopsis

Arguments

td Integer value that uniquely identifies a traffic domain. Minimum value: 1 Maximum value: 4094

Example

rm ns trafficDomain 1

unbind ns trafficDomain

Unbind vlan or bridgegroup entities from traffic domain NOTE: This command is deprecated.Traffic domains related configuration commands are being deprecated and will be removed in a future release. Citrix recommends you to use admin partitions instead of using traffic domains

Synopsis

Arguments

td Integer value that uniquely identifies a traffic domain. Minimum value: 1 Maximum value: 4094

vlan ID of the VLAN to bind to this traffic domain. More than one VLAN can be bound to a traffic domain, but the same VLAN cannot be a part of multiple traffic domains. Minimum value: 1 Maximum value: 4094

bridgegroup ID of the configured bridge to bind to this traffic domain. More than one bridge group can be bound to a traffic domain, but the same bridge group cannot be a part of multiple traffic domains. Minimum value: 1 Maximum value: 1000

vxlan ID of the VXLAN to bind to this traffic domain. More than one VXLAN can be bound to a traffic domain, but the same VXLAN cannot be a part of multiple traffic domains. Minimum value: 1 Maximum value: 16777215

Example

unbind ns trafficDomain 1 -vlan 2

bind ns trafficDomain

bind vlan or bridgegroup entities with traffic domain. NOTE: This command is deprecated.Traffic domains related configuration commands are being deprecated and will be removed in a future release. Citrix recommends you to use admin partitions instead of using traffic domains

Synopsis

Arguments

td Integer value that uniquely identifies a traffic domain. Minimum value: 1 Maximum value: 4094

vlan ID of the VLAN to bind to this traffic domain. More than one VLAN can be bound to a traffic domain, but the same VLAN cannot be a part of multiple traffic domains. Minimum value: 1 Maximum value: 4094

bridgegroup ID of the configured bridge to bind to this traffic domain. More than one bridge group can be bound to a traffic domain, but the same bridge group cannot be a part of multiple traffic domains. Minimum value: 1 Maximum value: 1000

vxlan ID of the VXLAN to bind to this traffic domain. More than one VXLAN can be bound to a traffic domain, but the same VXLAN cannot be a part of multiple traffic domains. Minimum value: 1 Maximum value: 16777215

Example

bind ns trafficDomain 1 -vlan 2

enable ns trafficDomain

Enable TrafficDomain. NOTE: This command is deprecated.Traffic domains related configuration commands are being deprecated and will be removed in a future release. Citrix recommends you to use admin partitions instead of using traffic domains

Synopsis

Arguments

td Integer value that uniquely identifies a traffic domain. Minimum value: 1 Maximum value: 4094

Example

enable ns trafficdomain 1

stat ns trafficDomain

Display statistics for Traffic Domains(s). NOTE: This command is deprecated.Traffic domains related configuration commands are being deprecated and will be removed in a future release. Citrix recommends you to use admin partitions instead of using traffic domains

Synopsis

Arguments

td An integer specifying the Traffic Domain ID. Possible values: 1 through 4094. Minimum value: 1 Maximum value: 4094

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Packets received (TdRxPkts) Packets received on this TD.

Packets sent (TdTxPkts) Packets transmitted from this TD.

Packets dropped (TdDropPkts) Inbound packets dropped on this TD by reception.

Example

stat ns trafficdomain 1

Related Commands

- stat ns partition

add ns trafficDomain

Configure Traffic Domain on the system. NOTE: This command is deprecated.Traffic domains related configuration commands are being deprecated and will be removed in a future release. Citrix recommends you to use admin partitions instead of using traffic domains

Synopsis

Arguments

td Integer value that uniquely identifies a traffic domain. Minimum value: 1 Maximum value: 4094

aliasName Name of traffic domain being added.

vmac Associate the traffic domain with a VMAC address instead of with VLANs. The Citrix ADC then sends the VMAC address of the traffic domain in all responses to ARP queries for network entities in that domain. As a result, the ADC can segregate subsequent incoming traffic for this traffic domain on the basis of the destination MAC address, because the destination MAC address is the VMAC address of the traffic domain. After creating entities on a traffic domain, you can easily manage and monitor them by performing traffic domain level operations.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

add ns trafficDomain 1 -aliasName td1

show ns trafficDomain

Display Traffic Domain configuration. NOTE: This command is deprecated.Traffic domains related configuration commands are being deprecated and will be removed in a future release. Citrix recommends you to use admin partitions instead of using traffic domains

Synopsis

Arguments

td Integer value that uniquely identifies a traffic domain. Minimum value: 1 Maximum value: 4094

Output

aliasName Name of traffic domain being added.

vmac Associate the traffic domain with a VMAC address instead of with VLANs. The Citrix ADC then sends the VMAC address of the traffic domain in all responses to ARP queries for network entities in that domain. As a result, the ADC can segregate subsequent incoming traffic for this traffic domain on the basis of the destination MAC address, because the destination MAC address is the VMAC address of the traffic domain. After creating entities on a traffic domain, you can easily manage and monitor them by performing traffic domain level operations.

stateflag Used internally for display.

vlan ID of the VLAN to bind to this traffic domain. More than one VLAN can be bound to a traffic domain, but the same VLAN cannot be a part of multiple traffic domains.

vxlan ID of the VXLAN to bind to this traffic domain. More than one VXLAN can be bound to a traffic domain, but the same VXLAN cannot be a part of multiple traffic domains.

bridgegroup ID of the configured bridge to bind to this traffic domain. More than one bridge group can be bound to a traffic domain, but the same bridge group cannot be a part of multiple traffic domains.

state The state of TrafficDmain.

devno count

Example

An example of the output of the show trafficDomain command is as follows:

1. ```
   Traffic Domain: 1

   Alias Name:     State: ENABLED

   Vlans : 50
   ```

2. ```
   Traffic Domain: 2

   Alias Name:     State: ENABLED

   Vlans : 2

   Bridge Group : 1
   ```

Done

clear ns trafficDomain

Remove Traffic Domain configuration. NOTE: This command is deprecated.This is deprecated as it is similar to rm traffidomain

Synopsis

Arguments

td Integer value that uniquely identifies a traffic domain. Minimum value: 1 Maximum value: 4094

ns-variable

The following operations can be performed on "ns-variable":

rm| add| set| unset| show|

rm ns variable

Remove a variable and its value(s).

Synopsis

rm ns variable <name>

Arguments

name Variable name. This follows the same syntax rules as other expression entity names: It must begin with an alpha character (A-Z or a-z) or an underscore (_). The rest of the characters must be alpha, numeric (0-9) or underscores. It cannot be re or xp (reserved for regular and XPath expressions). It cannot be an expression reserved word (e.g. SYS or HTTP). It cannot be used for an existing expression object (HTTP callout, patset, dataset, stringmap, or named expression).

Example

rm ns variable user_privilege_map

add ns variable

Create a variable for use in assignments and expressions.

Synopsis

add ns variable <name> -type <string>

Arguments

name Variable name. This follows the same syntax rules as other expression entity names: It must begin with an alpha character (A-Z or a-z) or an underscore (_). The rest of the characters must be alpha, numeric (0-9) or underscores. It cannot be re or xp (reserved for regular and XPath expressions). It cannot be an expression reserved word (e.g. SYS or HTTP). It cannot be used for an existing expression object (HTTP callout, patset, dataset, stringmap, or named expression).

type Specification of the variable type; one of the following: ulong - singleton variable with an unsigned 64-bit value. text(value-max-size) - singleton variable with a text string value. map(text(key-max-size),ulong,max-entries) - map of text string keys to unsigned 64-bit values. map(text(key-max-size),text(value-max-size),max-entries) - map of text string keys to text string values. where value-max-size is a positive integer that is the maximum number of bytes in a text string value. key-max-size is a positive integer that is the maximum number of bytes in a text string key. max-entries is a positive integer that is the maximum number of entries in a map variable. For a global singleton text variable, value-max-size <= 64000. For a global map with ulong values, key-max-size <= 64000. For a global map with text values, key-max-size + value-max-size <= 64000. max-entries is a positive integer that is the maximum number of entries in a map variable. This has a theoretical maximum of 2\^64-1, but in actual use will be much smaller, considering the memory available for use by the map. Example: map(text(10),text(20),100) specifies a map of text string keys (max size 10 bytes) to text string values (max size 20 bytes), with 100 max entries.

scope Scope of the variable: global - (default) one set of values visible across all Packet Engines on a standalone Citrix ADC, an HA pair, or all nodes of a cluster transaction - one value for each request-response transaction (singleton variables only; no expiration)

Possible values: global, transaction Default value: global

ifFull Action to perform if an assignment to a map exceeds its configured max-entries: lru - (default) reuse the least recently used entry in the map. undef - force the assignment to return an undefined (Undef) result to the policy executing the assignment.

Possible values: undef, lru Default value: lru

ifValueTooBig Action to perform if an value is assigned to a text variable that exceeds its configured max-size, or if a key is used that exceeds its configured max-size: truncate - (default) truncate the text string to the first max-size bytes and proceed. undef - force the assignment or expression evaluation to return an undefined (Undef) result to the policy executing the assignment or expression.

Possible values: undef, truncate Default value: truncate

ifNoValue Action to perform if on a variable reference in an expression if the variable is single-valued and uninitialized or if the variable is a map and there is no value for the specified key: init - (default) initialize the single-value variable, or create a map entry for the key and the initial value, using the -init value or its default. undef - force the expression evaluation to return an undefined (Undef) result to the policy executing the expression.

Possible values: undef, init Default value: init

init Initialization value for this variable, to which a singleton variable or map entry will be set if it is referenced before an assignment action has assigned it a value. If the singleton variable or map entry already has been assigned a value, setting this parameter will have no effect on that variable value. Default: 0 for ulong, NULL for text

expires Value expiration in seconds. If the value is not referenced within the expiration period it will be deleted. 0 (the default) means no expiration. Minimum value: 0 Maximum value: 31622400

comment Comments associated with this variable.

Example

add ns variable user_privilege_map -type map(text(15),text(10),10000)

set ns variable

Set a variable for use in assignments and expressions.

Synopsis

set ns variable <name>

Arguments

name Variable name. This follows the same syntax rules as other expression entity names: It must begin with an alpha character (A-Z or a-z) or an underscore (_). The rest of the characters must be alpha, numeric (0-9) or underscores. It cannot be re or xp (reserved for regular and XPath expressions). It cannot be an expression reserved word (e.g. SYS or HTTP). It cannot be used for an existing expression object (HTTP callout, patset, dataset, stringmap, or named expression).

type Specification of the variable type; one of the following: ulong - singleton variable with an unsigned 64-bit value. text(value-max-size) - singleton variable with a text string value. map(text(key-max-size),ulong,max-entries) - map of text string keys to unsigned 64-bit values. map(text(key-max-size),text(value-max-size),max-entries) - map of text string keys to text string values. where value-max-size is a positive integer that is the maximum number of bytes in a text string value. key-max-size is a positive integer that is the maximum number of bytes in a text string key. max-entries is a positive integer that is the maximum number of entries in a map variable. For a global singleton text variable, value-max-size <= 64000. For a global map with ulong values, key-max-size <= 64000. For a global map with text values, key-max-size + value-max-size <= 64000. max-entries is a positive integer that is the maximum number of entries in a map variable. This has a theoretical maximum of 2\^64-1, but in actual use will be much smaller, considering the memory available for use by the map. Example: map(text(10),text(20),100) specifies a map of text string keys (max size 10 bytes) to text string values (max size 20 bytes), with 100 max entries.

ifFull Action to perform if an assignment to a map exceeds its configured max-entries: lru - (default) reuse the least recently used entry in the map. undef - force the assignment to return an undefined (Undef) result to the policy executing the assignment.

Possible values: undef, lru Default value: lru

ifValueTooBig Action to perform if an value is assigned to a text variable that exceeds its configured max-size, or if a key is used that exceeds its configured max-size: truncate - (default) truncate the text string to the first max-size bytes and proceed. undef - force the assignment or expression evaluation to return an undefined (Undef) result to the policy executing the assignment or expression.

Possible values: undef, truncate Default value: truncate

ifNoValue Action to perform if on a variable reference in an expression if the variable is single-valued and uninitialized or if the variable is a map and there is no value for the specified key: init - (default) initialize the single-value variable, or create a map entry for the key and the initial value, using the -init value or its default. undef - force the expression evaluation to return an undefined (Undef) result to the policy executing the expression.

Possible values: undef, init Default value: init

init Initialization value for this variable, to which a singleton variable or map entry will be set if it is referenced before an assignment action has assigned it a value. If the singleton variable or map entry already has been assigned a value, setting this parameter will have no effect on that variable value. Default: 0 for ulong, NULL for text

expires Value expiration in seconds. If the value is not referenced within the expiration period it will be deleted. 0 (the default) means no expiration. Minimum value: 0 Maximum value: 31622400

comment Comments associated with this variable.

Example

set ns variable user_privilege_map -type map(text(15),text(10),10000)

unset ns variable

Use this command to remove ns variable settings.Refer to the set ns variable command for meanings of the arguments.

Synopsis

unset ns variable <name>

show ns variable

Display configured variables

Synopsis

show ns variable

Arguments

name Variable name. This follows the same syntax rules as other expression entity names: It must begin with an alpha character (A-Z or a-z) or an underscore (_). The rest of the characters must be

alpha, numeric (0-9) or underscores. It cannot be re or xp (reserved for regular and XPath expressions). It cannot be an expression reserved word (e.g. SYS or HTTP). It cannot be used for an existing expression object (HTTP callout, patset, dataset, stringmap, or named expression).

Output

type Specification of the variable type; one of the following: ulong - singleton variable with an unsigned 64-bit value. text(value-max-size) - singleton variable with a text string value. map(text(key-max-size),ulong,max-entries) - map of text string keys to unsigned 64-bit values. map(text(key-max-size),text(value-max-size),max-entries) - map of text string keys to text string values. where value-max-size is a positive integer that is the maximum number of bytes in a text string value. key-max-size is a positive integer that is the maximum number of bytes in a text string key. max-entries is a positive integer that is the maximum number of entries in a map variable. For a global singleton text variable, value-max-size ' 64000. For a global map with ulong values, key-max-size ' 64000. For a global map with text values, key-max-size + value-max-size ' 64000. max-entries is a positive integer that is the maximum number of entries in a map variable. This has a theoretical maximum of 2\^64-1, but in actual use will be much smaller, considering the memory available for use by the map. Example: map(text(10),text(20),100) specifies a map of text string keys (max size 10 bytes) to text string values (max size 20 bytes), with 100 max entries.

scope Scope of the variable: global - (default) one set of values visible across all Packet Engines on a standalone Citrix ADC, an HA pair, or all nodes of a cluster transaction - one value for each request-response transaction (singleton variables only; no expiration)

ifFull Action to perform if an assignment to a map exceeds its configured max-entries: lru - (default) reuse the least recently used entry in the map. undef - force the assignment to return an undefined (Undef) result to the policy executing the assignment.

ifValueTooBig Action to perform if an value is assigned to a text variable that exceeds its configured max-size, or if a key is used that exceeds its configured max-size: truncate - (default) truncate the text string to the first max-size bytes and proceed. undef - force the assignment or expression evaluation to return an undefined (Undef) result to the policy executing the assignment or expression.

ifNoValue Action to perform if on a variable reference in an expression if the variable is single-valued and uninitialized or if the variable is a map and there is no value for the specified key: init - (default) initialize the single-value variable, or create a map entry for the key and the initial value, using the -init value or its default. undef - force the expression evaluation to return an undefined (Undef) result to the policy executing the expression.

expires Value expiration in seconds. If the value is not referenced within the expiration period it will be deleted. 0 (the default) means no expiration.

init Initialization value for this variable, to which a singleton variable or map entry will be set if it is referenced before an assignment action has assigned it a value. If the singleton variable or map entry already has been assigned a value, setting this parameter will have no effect on that variable value. Default: 0 for ulong, NULL for text

comment Comments associated with this variable.

builtin Flag to determine if the variable is built-in or not

feature The feature to be checked while applying this config

referenceCount The number of references to the variable in expressions and assignments.

stateflag devno count

ns-version

The following operations can be performed on "ns-version":

show ns version

Displays the version and build number of the appliance.

Synopsis

show ns version

Arguments

installedversion Installed version

Output

version Version.

Mode Kernel mode (KMPE/VMPE).

ns-vpxparam

The following operations can be performed on "ns-vpxparam":

show| set| unset|

show ns vpxparam

Display the vpx configuration setting for the vpx.

Synopsis

show ns vpxparam

Arguments

Output

cpuyield Display the vCPU yield setting. In a virtual appliance, CPU yield attribute will release the CPU processing for other virtual appliances on the same platform.

ownerNode ID of the cluster node for which you are setting the cpuyield and/or KVMVirtioMultiqueue. It can be configured only through the cluster IP address.

masterclockcpu1 Display master clock source. This attribute is set to YES if clock source is cpu1 and NO for cpu0.

VPXEnvironment Shows VPX Running Environmentrunning 0 VPX ON PREM, 1 AWS, 2 OPENSTACK 3 Azure, 4 GCP CLoud

MemoryStatus Provides the information about memory status

CloudProductCode Cloud Product Code Description .

VpxOEMCode OEM Distribution Code.

TechnicalSupportPIN Technical Support PIN for cloud subscription VMs.

KVMVirtioMultiqueue This setting applicable on KVM VPX with virtio NICs, is to configure multiple queues for all virtio interfaces.

- There are 2 options for this behavior:

1. YES - Allows VPX to use multiple queues for each virtio interface as configured through the KVM Hypervisor.
2. NO - Each virtio interface within VPX will use a single queue for transmit and receive.

- Its behavior in different scenarios:

1. As this setting is node specific only, it will not be propagated to other nodes, when executed on Cluster(CLIP) and HA(Primary).

2. In cluster setup, use '-ownerNode' to specify ID of the cluster node.

devno count stateflag

set ns vpxparam

Set vpx configuration settings for the existing vpx.

Synopsis

set ns vpxparam

Arguments

cpuyield This setting applicable in virtual appliances, is to affect the cpu yield(relinquishing the cpu resources) in any hypervised environment.

- There are 3 options for the behavior:

1. YES - Allow the Virtual Appliance to yield its vCPUs periodically, if there is no data traffic.
2. NO - Virtual Appliance will not yield the vCPU.
3. DEFAULT - Restores the default behaviour, according to the license.

- Its behavior in different scenarios:

1. As this setting is node specific only, it will not be propagated to other nodes, when executed on Cluster(CLIP) and HA(Primary).
2. In cluster setup, use '-ownerNode' to specify ID of the cluster node.
3. This setting is a system wide implementation and not granular to vCPUs.
4. No effect on the management PE.

Possible values: DEFAULT, YES, NO Default value: DEFAULT

ownerNode ID of the cluster node for which you are setting the cpuyield and/or KVMVirtioMultiqueue. It can be configured only through the cluster IP address. Default value: 255 Minimum value: 0 Maximum value: 31

KVMVirtioMultiqueue This setting applicable on KVM VPX with virtio NICs, is to configure multiple queues for all virtio interfaces.

- There are 2 options for this behavior:

1. YES - Allows VPX to use multiple queues for each virtio interface as configured through the KVM Hypervisor.
2. NO - Each virtio interface within VPX will use a single queue for transmit and receive.

- Its behavior in different scenarios:

1. As this setting is node specific only, it will not be propagated to other nodes, when executed on Cluster(CLIP) and HA(Primary).
2. In cluster setup, use '-ownerNode' to specify ID of the cluster node.

Possible values: YES, NO Default value: NO

Example

set ns vpxparam -cpuyield YES/NO/DEFAULT

unset ns vpxparam

Use this command to remove ns vpxparam settings.Refer to the set ns vpxparam command for meanings of the arguments.

Synopsis

unset ns vpxparam

ns-weblogparam

The following operations can be performed on "ns-weblogparam":

unset| set| show|

unset ns weblogparam

Use this command to remove ns weblogparam settings.Refer to the set ns weblogparam command for meanings of the arguments.

Synopsis

unset ns weblogparam

set ns weblogparam

Sets the Weblog parameters.

Synopsis

set ns weblogparam

Arguments

bufferSizeMB Buffer size, in MB, allocated for log transaction data on the system. The maximum value is limited to the memory available on the system. Default value: 16 Minimum value: 1 Maximum value: 4294967294LU

customReqHdrs Name(s) of HTTP request headers whose values should be exported by the Web Logging feature.

customRspHdrs Name(s) of HTTP response headers whose values should be exported by the Web Logging feature.

show ns weblogparam

Displays the Weblog parameters.

Synopsis

show ns weblogparam

Arguments

Output

bufferSizeMB Buffer size in MB.

customReqHdrs Name(s) of HTTP request headers whose values should be exported by the Web Logging feature.

customRspHdrs Name(s) of HTTP response headers whose values should be exported by the Web Logging feature.

builtin Flag to determine if log bufs is built-in or not

feature The feature to be checked while applying this config

ns-xmlnamespace

The following operations can be performed on "ns-xmlnamespace":

set| add| rm| unset| show|

set ns xmlnamespace

Modifies the mapping between an XML prefix and a namespace URI.

Synopsis

set ns xmlnamespace <prefix>

Arguments

prefix XML prefix for which the namespace or description must be added or updated.

namespace Expanded namespace for which the XML prefix is provided.

description Description for the prefix.

Example

set ns xmlnamespace soap -description SOAP/1.1

add ns xmlnamespace

Adds a mapping between an XML prefix and a namespace URI (Uniform Resource Identifier).

Synopsis

add ns xmlnamespace <prefix> <namespace>

Arguments

prefix XML prefix.

namespace Expanded namespace for which the XML prefix is provided.

description Description for the prefix.

Example

add ns xmlnamespace soap http://schemas.xmlsoap.org/soap/envelope/

rm ns xmlnamespace

Removes the mapping between an XML prefix and a namespace URI.

Synopsis

rm ns xmlnamespace <prefix>

Arguments

prefix XML prefix for which the mapping must be removed.

Example

rm ns xmlnamespace soap

unset ns xmlnamespace

Use this command to remove ns xmlnamespace settings.Refer to the set ns xmlnamespace command for meanings of the arguments.

Synopsis

unset ns xmlnamespace <prefix>

show ns xmlnamespace

Displays the mappings between XML prefixes to namespace URIs.

Synopsis

show ns xmlnamespace

Arguments

prefix Name of the prefix for which the mappings must be displayed.

Output

namespace Expanded namespace for which the XML prefix is provided.

description Description for the prefix.

devno count stateflag

Example

show ns xmlnamespace soap

ns

The following operations can be performed on "ns":

stat| config|

stat ns

Displays generic statistics of the Citrix ADC.

Synopsis

stat ns

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Average CPU usage (%) (CPU) Average CPU utilization percentage. Not applicable for a single-CPU system.

CPU usage (%) (CPU) CPU utilization percentage.

Maximum memory(KB) Deprecated (MaxMem) Largest amount of memory the Citrix ADC can dedicate to caching, up to 50% of available memory. A 0 value disables caching, but the caching module continues to run.

Delta compression ratio (DlCmpRt) Ratio of compressible data received to compressed data transmitted.If this ratio is one (uncmp:1.0) that means compression is disabled or we are not able to compress even a single compressible packet.

Average CPU usage (CPU) Shows average CPU utilization percentage if more than 1 CPU is present.

CPU usage (CPU) CPU utilization percentage.

Memory usage (MemUsage) Percentage of memory utilization on Citrix ADC.

Total HTTP compression ratio Ratio of total HTTP data received to total HTTP data transmitted.

HTTP compression ratio Ratio of the compressible data received from the server to the compressed data sent to the client.

Utilized memory(KB) (UtiMem) Amount of memory the integrated cache is currently using.

Maximum memory active value(KB) (MaxMemActive) Currently active value of maximum memory

Maximum memory(KB) (Max64Mem) Largest amount of memory the Citrix ADC can dedicate to caching, up to 50% of available memory. A 0 value disables caching, but the caching module continues to run.

Origin bandwidth saved(%) (POrBan) Percentage of origin bandwidth saved, expressed as number of bytes served from the integrated cache divided by all bytes served. The assumption is that all compression is done in the Citrix ADC.

Misses (TotMiss) Intercepted HTTP requests requiring fetches from origin server.

Hits (TotHit) Responses served from the integrated cache. These responses match a policy with a CACHE action.

InUse Memory (%) (MemUsage) Percentage of memory utilization on Citrix ADC.

Memory usage (MB) (MemUseMB) Main memory currently in use, in megabytes.

Management CPU usage (%) (CPU) Average Management CPU utilization percentage.

Packet CPU usage (%) (CPU) Average CPU utilization percentage for all packet engines excluding management PE.

Up since(Local) (Since) Time (in local timezone format) when the Citrix ADC was last started.

Up since (Since) Time when the Citrix ADC was last started.

Last Transition time (TransTime) Time when the last master state transition occurred. You can use this statistic for debugging.

System state (HAState) State of the HA node, based on its health, in a high availability setup. Possible values are: UP - Indicates that the node is accessible and can function as either a primary or secondary node. DISABLED - Indicates that the high availability status of the node has been manually disabled. Synchronization and propagation cannot take place between the peer nodes. INIT - Indicates that the node is in the process of becoming part of the high availability configuration. PARTIALFAIL - Indicates that one of the high availability monitored interfaces has failed because of a card or link failure. This state triggers a failover. COMPLETEFAIL - Indicates that all the interfaces of the node are unusable, because the interfaces on which high availability monitoring is enabled are not connected or are manually disabled. This state triggers a failover. DUMB - Indicates that the node is in listening mode. It does not participate in high availability transitions or transfer configuration from the peer node. This is a configured value, not a statistic. PARTIALFAILSSL - Indicates that the SSL card has failed. This state triggers a failover. ROUTEMONITORFAIL - Indicates that the route monitor has failed. This state triggers a failover.

Master state (mastate) Indicates the high availability state of the node. Possible values are: STAYSECONDARY - Indicates that the selected node remains the secondary node in a high availability setup. In this case a forced failover does not change the state but, instead, returns an appropriate error message. This is a configured value and not a statistic. PRIMARY - Indicates that the selected node is the primary node in a high availability setup. SECONDARY - Indicates that the selected node is the secondary node in a high availability setup. CLAIMING - Indicates that the secondary node is in the process of taking over as the primary node. This is the intermediate state in the transition of the secondary node to primary status. FORCE CHANGE - Indicates that the secondary node is forcibly changing its status to primary due to a forced failover issued on the secondary node.

 # SSL cards UP (SSLCardUP) Number of SSL cards that are UP. If the number of cards UP is lower than a threshold, a failover is initiated.

 # SSL cards present (SSLCards) Number of SSL crypto cards present on the Citrix ADC.

/flash Used (%) (disk0PerUsage) Used space in /flash partition of the disk, as a percentage. This is a critical counter. You can configure /flash Used (%) by using the Set snmp alarm DISK-USAGE-HIGH command.

/var Used (%) (disk1PerUsage) Used space in /var partition of the disk, as a percentage. This is a critical counter. You can configure /var Used (%) by using the Set snmp alarm DISK-USAGE-HIGH command.

/flash Available (MB) (disk0Avail) Available space in /flash partition of the hard disk.

/var Available (MB) (disk1Avail) Available space in /var partition of the hard disk.

Megabits received (RxMb) Number of megabytes received by the Citrix ADC.

Megabits transmitted (TxMb) Number of megabytes transmitted by the Citrix ADC.

All client connections (CltCx) Client connections, including connections in the Opening, Established, and Closing state.

Established client connections (CltCxE) Current client connections in the Established state, which indicates that data transfer can occur between the Citrix ADC and the client.

All server connections (SvrCx) Server connections, including connections in the Opening, Established, and Closing state.

Established server connections (SvrCxE) Current server connections in the Established state, which indicates that data transfer can occur between the Citrix ADC and the server.

Total requests (HTReqRx) Total number of HTTP requests received.

Total responses (HTRspRx) Total number of HTTP responses sent.

Request bytes received (HTReqbRx) Total number of bytes of HTTP request data received.

Response bytes received (HTRspbRx) Total number of bytes of HTTP response data received.

SSL transactions (SSLTrn) Number of SSL transactions on the Citrix ADC

SSL session hits (SeHit) Number of SSL session reuse hits on the Citrix ADC.

requests (reqs) HTTP/HTTPS requests sent to your protected web servers via the Application Firewall.

responses (resps) HTTP/HTTPS responses sent by your protected web servers via the Application Firewall.

aborts Incomplete HTTP/HTTPS requests aborted by the client before the Application Firewall could finish processing them.

redirects (redirect) HTTP/HTTPS requests redirected by the Application Firewall to a different Web page or web server. (HTTP 302)

Inbound BW Limits Exceeded (BWInExc) Inbound BW Limits Exceeded

Outbound BW Limits Exceeded (BWOutExc) Outbound BW Limits Exceeded

PPS Limits Exceeded (PPSExc) PPS Limits Exceeded

Conn-Tracking Limits Exceeded (ConnExc) Conn-Tracking Limits Exceeded

Link-Local Limits Exceeded (LocalExc) Link-Local Limits Exceeded

Misc. Counter 0 (misc0) Miscellaneous Counter 0.

Misc. Counter 1 (misc1) Miscellaneous Counter 1.

CPU usage (CPU) CPU utilization: percentage * 10.

Management CPU usage (CPU) Management CPU utilization: percentage * 10.

304 hits (304Hit) Object not modified responses served from the cache. (Status code 304 served instead of the full response.)

Non-304 hits (Non304Hit) Total number of full (non-304) responses served from the cache. A 304 status code indicates that a response has not been modified since the last time it was served

sql hits (sqlHit) sql response served from cache

Requests (CacReq) Total cache hits plus total cache misses.

Compressed bytes transmitted Number of bytes the Citrix ADC sends to the client after compressing the response from the server.

Compressible bytes received Number of bytes that can be compressed, which the Citrix ADC receives from the server. This gives the content length of the response that the Citrix ADC receives from server.

Compressible bytes received (DlCmpRxB) Total number of delta-compressible bytes received by Citrix ADC.

Compressed bytes transmitted (DlCmpTxB) Total number of delta-compressed bytes transmitted by Citrix ADC.

Related Commands

- stat ns partition

config ns

Displays a menu to configure the basic parameters of a Citrix ADC. Note: The appliance must be rebooted for these changes to take effect.

Synopsis

config ns

Arguments

reboot

The following operations can be performed on "reboot":

reboot

Restarts the Citrix ADC. Note:

- When a standalone Citrix ADC is rebooted, the unsaved configurations (configurations performed since the last 'save ns config' command was issued) are lost.
- In the high availability mode, when the primary appliance is rebooted, the secondary system takes over and becomes the primary. The unsaved configurations from the old primary are available on the new primary appliance.
- In a cluster setup, this command can be executed only through the cluster IP address and it reboots only the configuration coordinator.

Synopsis

reboot

Arguments

warm Restarts the Citrix ADC software without rebooting the underlying operating system. The session terminates and you must log on to the appliance after it has restarted. Note: This argument is required only for nCore appliances. Classic appliances ignore this argument.

shutdown

The following operations can be performed on "shutdown":

shutdown

Stops all operations and powers off the Citrix ADC. Note:

- When a standalone Citrix ADC is shut down, the unsaved configurations (configurations performed since the last 'save ns config' command was issued) are lost.

- In a high availability setup, when the primary appliance is shut down, the secondary appliance takes over and becomes the primary. The unsaved configurations from the old primary are available on the new primary appliance.
- In a cluster setup, this command can be executed only through the cluster IP address and it shuts down only the configuration coordinator.

Synopsis

shutdown

Arguments

ntp

Ntp

The entities on which you can perform NetScaler CLI operations:

- ntp-param
- ntp-server
- ntp-status
- ntp-sync

ntp-param

The following operations can be performed on "ntp-param":

unset| set| show|

unset ntp param

Use this command to remove ntp param settings.Refer to the set ntp param command for meanings of the arguments.

Synopsis

unset ntp param

set ntp param

Modifies the values for NTP parameters on the Citrix ADC.

Synopsis

set ntp param

Arguments

authentication Apply NTP authentication, which enables the NTP client (Citrix ADC) to verify that the server is in fact known and trusted.

Possible values: YES, NO Default value: YES

trustedkey Key identifiers that are trusted for server authentication with symmetric key cryptography in the keys file. Minimum value: 1 Maximum value: 65534

autokeyLogsec Autokey protocol requires the keys to be refreshed periodically. This parameter specifies the interval between regenerations of new session keys. In seconds, expressed as a power of 2. Default value: 12 Minimum value: 0 Maximum value: 32

revokeLogsec Interval between re-randomizations of the autokey seeds to prevent brute-force attacks on the autokey algorithms. Default value: 16 Minimum value: 0 Maximum value: 32

show ntp param

Displays information about the NTP parameters.

Synopsis

show ntp param

Arguments

Output

authentication Apply NTP authentication, which enables the NTP client (Citrix ADC) to verify that the server is in fact known and trusted.

trustedkey Key identifiers that are trusted for server authentication with symmetric key cryptography in the keys file.

autokeyLogsec Autokey protocol requires the keys to be refreshed periodically. This parameter specifies the interval between regenerations of new session keys. In seconds, expressed as a power of 2.

revokeLogsec Interval between re-randomizations of the autokey seeds to prevent brute-force attacks on the autokey algorithms.

ntp-server

The following operations can be performed on "ntp-server":

show| set| rm| unset| add|

show ntp server

Displays information about an NTP server. You can specify the server by IP address or by name.

Synopsis

show ntp server

Arguments

serverIP IP address of the NTP server about which to display information.

serverName Name of the NTP server about which to display information.

Output

minpoll Minimum poll interval of the server in secs.

maxpoll Maximum poll interval of the server in secs.

preferredNtpServer Preferred NTP server. The Citrix ADC chooses this NTP server for time synchronization among a set of correctly operating hosts.

autokey Use the Autokey protocol for key management for this server, with the cryptographic values (for example, symmetric key, host and public certificate files, and sign key) generated by the ntp-keygen utility. To require authentication for communication with the server, you must set either the value of this parameter or the key parameter.

key Key to use for encrypting authentication fields. All packets sent to and received from the server must include authentication fields encrypted by using this key. To require authentication for communication with the server, you must set either the value of this parameter or the autokey parameter.

devno count stateflag

set ntp server

Modifies the specified attributes of an NTP server.

Synopsis

set ntp server (<serverIP> | <serverName>)

Arguments

serverIP IP address of the NTP server to be modified.

serverName Name of the NTP server to be modified.

minpoll Minimum time after which the NTP server must poll the NTP messages. In seconds, expressed as a power of 2. Default value: NS_NTP_MINPOLL_DEFAULT_VALUE Minimum value: 4 Maximum value: 17

maxpoll Maximum time after which the NTP server must poll the NTP messages. In seconds, expressed as a power of 2. Default value: NS_NTP_MAXPOLL_DEFAULT_VALUE Minimum value: 4 Maximum value: 17

preferredNtpServer Preferred NTP server. The Citrix ADC chooses this NTP server for time synchronization among a set of correctly operating hosts.

Possible values: YES, NO Default value: NO

autokey Use the Autokey protocol for key management for this server, with the cryptographic values (for example, symmetric key, host and public certificate files, and sign key) generated by the ntp-keygen utility. To require authentication for communication with the server, you must set either the value of this parameter or the key parameter.

key Key to use for encrypting authentication fields. All packets sent to and received from the server must include authentication fields encrypted by using this key. To require authentication for communication with the server, you must set either the value of this parameter or the autokey parameter. Minimum value: 1 Maximum value: 65534

rm ntp server

Removes an NTP server. You can specify the server by IP address or by name.

Synopsis

rm ntp server (<serverIP> | <serverName>)

Arguments

serverIP IP address of the NTP server to be removed.

serverName Name of the NTP server to be removed.

unset ntp server

Unset the specified attributes of an NTP server..Refer to the set ntp server command for meanings of the arguments.

Synopsis

unset ntp server (<serverIP> | <serverName>)

add ntp server

Adds an NTP server to the appliance. This server can be used to synchronize the time on the appliance to the network time.

Synopsis

add ntp server (<serverIP> | <serverName>)

Arguments

serverIP IP address of the NTP server.

serverName Fully qualified domain name of the NTP server.

minpoll Minimum time after which the NTP server must poll the NTP messages. In seconds, expressed as a power of 2. Default value: NS_NTP_MINPOLL_DEFAULT_VALUE Minimum value: 4 Maximum value: 17

maxpoll Maximum time after which the NTP server must poll the NTP messages. In seconds, expressed as a power of 2. Default value: NS_NTP_MAXPOLL_DEFAULT_VALUE Minimum value: 4 Maximum value: 17

autokey Use the Autokey protocol for key management for this server, with the cryptographic values (for example, symmetric key, host and public certificate files, and sign key) generated by the ntp-keygen utility. To require authentication for communication with the server, you must set either the value of this parameter or the key parameter.

key Key to use for encrypting authentication fields. All packets sent to and received from the server must include authentication fields encrypted by using this key. To require authentication for communication with the server, you must set either the value of this parameter or the autokey parameter. Minimum value: 1 Maximum value: 65534

ntp-status

The following operations can be performed on "ntp-status":

show ntp status

Displays a list of the peers known to the server and a summary of their state.

Synopsis

show ntp status

Output

response

ntp-sync

The following operations can be performed on "ntp-sync":

disable| show| enable|

disable ntp sync

Disables NTP synchronization.

Synopsis

disable ntp sync

show ntp sync

Displays the status of the NTP synchronization.

Synopsis

show ntp sync

Arguments

Output

state Show NTP status

enable ntp sync

Enables NTP synchronization. When NTP synchronization is enabled, the NTP daemon is spawned for time synchronization.

Synopsis

enable ntp sync

pcp

Pcp

The entities on which you can perform NetScaler CLI operations:

- pcp-map
- pcp-profile
- pcp-server

pcp-map

The following operations can be performed on "pcp-map":

show pcp map

Displays the maps created by pcp server.

Synopsis

show pcp map

Arguments

NatType Type of sessions to be displayed.

Possible values: NAT44, DS-Lite, NAT64 Default value: NAT44

Output

pcpSrcIP Internal IP address

subscrIP IPV4 src address of Client in DS-Lite

pcpSrcPort Internal Port

pcpDstIP Remote PEER IP address

pcpDstPort Remote PEER Port

pcpNatIP External IP address

pcpNatPort External Port Number

pcpProtocol Protocol of the PCP mapping

pcpAddr Address of PCP Map entity.

pcpNounce PCP Mapping Nounce

pcpRefcnt Refcount, which indicates how many session is active.

pcpLifeTime Integer value that shows the requested lifetime.

devno count stateflag

pcp-profile

The following operations can be performed on "pcp-profile":

add| unset| set| show| rm|

add pcp profile

Creates a pcp profile.

Synopsis

add pcp profile <name>

Arguments

name Name for the PCP Profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my pcpProfile" or my pcpProfile).

mapping This argument is for enabling/disabling the MAP opcode of current PCP Profile

Possible values: ENABLED, DISABLED Default value: ENABLED

peer This argument is for enabling/disabling the PEER opcode of current PCP Profile

Possible values: ENABLED, DISABLED Default value: ENABLED

minMapLife Integer value that identify the minimum mapping lifetime (in seconds) for a pcp profile. default(120s) Minimum value: 1 Maximum value: 2147483647

maxMapLife Integer value that identify the maximum mapping lifetime (in seconds) for a pcp profile. default(86400s = 24Hours). Minimum value: 1 Maximum value: 2147483647

announceMultiCount Integer value that identify the number announce message to be send. Default value: 10 Minimum value: 0 Maximum value: 65535

thirdParty This argument is for enabling/disabling the THIRD PARTY opcode of current PCP Profile

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

add pcp profile prof1

unset pcp profile

Use this command to remove pcp profile settings.Refer to the set pcp profile command for meanings of the arguments.

Synopsis

unset pcp profile <name>

set pcp profile

Modifies the specified parameters of a pcp profile.

Synopsis

set pcp profile <name>

Arguments

name Name for the PCP Profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my pcpProfile" or my pcpProfile).

mapping This argument is for enabling/disabling the MAP opcode of current PCP Profile

Possible values: ENABLED, DISABLED Default value: ENABLED

peer This argument is for enabling/disabling the PEER opcode of current PCP Profile

Possible values: ENABLED, DISABLED Default value: ENABLED

minMapLife Integer value that identify the minimum mapping lifetime (in seconds) for a pcp profile. default(120s) Minimum value: 1 Maximum value: 2147483647

maxMapLife Integer value that identify the maximum mapping lifetime (in seconds) for a pcp profile. default(86400s = 24Hours). Minimum value: 1 Maximum value: 2147483647

announceMultiCount Integer value that identify the number announce message to be send. Default value: 10 Minimum value: 0 Maximum value: 65535

thirdParty This argument is for enabling/disabling the THIRD PARTY opcode of current PCP Profile

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set pcp profile prof1 -MAPPING ENABLED

show pcp profile

Displays the pcp server information.

Synopsis

show pcp profile

Arguments

name Name of the pcp server.

Output

mapping This argument is for enabling/disabling the MAP opcode of current PCP Profile

peer This argument is for enabling/disabling the PEER opcode of current PCP Profile

minMapLife Integer value that identify the minimum mapping lifetime (in seconds) for a pcp profile. default(120s)

maxMapLife Integer value that identify the maximum mapping lifetime (in seconds) for a pcp profile. default(86400s = 24Hours).

announceMultiCount Integer value that identify the number announce message to be send.

thirdParty This argument is for enabling/disabling the THIRD PARTY opcode of current PCP Profile

devno count stateflag

rm pcp profile

Removes a pcp profile from the Citrix ADC.

Synopsis

rm pcp profile <name>@ ...

Arguments

name Name of the pcp server.

Example

rm pcp profile prof1

pcp-server

The following operations can be performed on "pcp-server":

set| show| add| unset| rm| stat|

set pcp server

Modifies the specified parameters of a pcp server.

Synopsis

set pcp server <name>

Arguments

name Name of the pcp server.

port Port number for the PCP server. Default value: 5351

pcpProfile pcp profile name

Example

set pcp server pcp_svr -port 5000 -profile profile_1

show pcp server

Displays the pcp server information.

Synopsis

show pcp server

Arguments

name Name of the pcp server.

Output

IPAddress The IP address of the PCP server.

port Port number for the PCP server.

pcpProfile pcp profile name

devno count stateflag

add pcp server

Creates a pcp server.

Synopsis

add pcp server <name> <IPAddress>

Arguments

name Name for the PCP server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my pcpServer" or my pcpServer).

IPAddress The IP address of the PCP server.

port Port number for the PCP server. Default value: 5351

pcpProfile pcp profile name

Example

add pcp server pcp_svr 10.102.1.10

unset pcp server

Use this command to remove pcp server settings.Refer to the set pcp server command for meanings of the arguments.

Synopsis

unset pcp server <name>

rm pcp server

Removes a pcp server from the Citrix ADC.

Synopsis

rm pcp server <name> ...

Arguments

name Name of the pcp server.

Example

rm pcp server pcp_svr

stat pcp server

DIsplay pcp statistics.

Synopsis

stat pcp server

Arguments

name PCP Statistics per Server

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Total PCP Requests received (requests) PCP Request received.

Total Responses sent (responses) Number PCP responces sent.

Total PCP MAP Rquests rcvd (peerReq) PCP MAP Requests received.

Total PCP PEER Requests rcvd (mapRqsts) PCP PEER Requests received.

Total requests with errors (errInReq) total PCP request with error.

Total responses with errors (errInRes) Total PCP responses with errors.

Total unsupported version request (unsuppVers) PCP request with unsupported version.

Total Malformed Requests (malformedReq) total PCP request having malformed PCP packets.

Total Unsupported OPCODES (unsupOpcode) total Unsupproted OPCODES received Requests.

Total Unsupported OPTIONS (unsupOption) total Unsupproted OPTIONS received in requests.

Total malformed OPTIONS (malformedOption) total malformed OPTIONS received in requests.

Total Network Failures (ntwrkFail) Total Network Failures.

Total No resources reponse (noResource) no resources

Total Unsupported Protocols requests (unsupProto) Total Unsupported Protocols requests.

Total User Ex Qouta (userExqouta) Total user ex quota.

Total cannot provide extrnl resp (noExternal) Total responses with opcode can not provide external.

Total address mismatch rqsts (addrMismatch) Total address mismatch.

Total Excess Remote Peers (excessPeers) Total responses with opcode excessive remote peers.

policy

Policy

The entities on which you can perform NetScaler CLI operations:

- policy-dataset
- policy-evaluation
- policy-expression
- policy-httpCallout
- policy-map
- policy-param
- policy-patset
- policy-patsetFile
- policy-stringmap
- policy-urlset

policy-dataset

The following operations can be performed on "policy-dataset":

show| rm| add| bind| unbind|

show policy dataset

Display the configured dataset(s).

Synopsis

show policy dataset

Arguments

name Name of the dataset. Must not exceed 127 characters.

Output

stateflag value Value of the specified type that is associated with the dataset. For ipv4 and ipv6, value can be a subnet using the slash notation address/n, where address is the beginning of the subnet and n is the number of left-most bits set in the subnet mask, defining the end of the subnet. The start address will be masked by the subnet mask if necessary, for example for 192.128.128.0/10, the start address will be 192.128.0.0.

endRange The dataset entry is a range from <value> through <end_range>, inclusive. endRange cannot be used if value is an ipv4 or ipv6 subnet and endRange cannot itself be a subnet.

index The index of the value (ipv4, ipv6, number) associated with the set.

type Type of value to bind to the dataset.

MaxIndex Maximum number of values bounded to dataset. The maxindex value will not be decreased when we unbind a value from the dataset. This field is used in auto-generated indexing type.

comment Any comments to preserve information about this dataset or a data bound to this dataset.

patsetFile File which contains list of patterns that needs to be bound to the dataset. A patsetfile cannot be associated with multiple datasets.

devno count

Example

show policy dataset set1

rm policy dataset

Removes a dataset from the appliance.

Synopsis

rm policy dataset <name>

Arguments

name Name of the dataset to remove.

Example

rm policy dataset pat1

add policy dataset

Adds a policy dataset to the appliance. The patset file option can be used to bind the patterns contained in a file, which is imported from Citrix ADC or from an external location (please check import/add/update patsetfile). A dataset can be configured with at most one patsetfile!

Synopsis

add policy dataset <name> <type>

Arguments

name Name of the dataset. Must not exceed 127 characters.

type Type of value to bind to the dataset.

Possible values: ipv4, number, ipv6, ulong, double, mac

comment Any comments to preserve information about this dataset or a data bound to this dataset.

patsetFile File which contains list of patterns that needs to be bound to the dataset. A patsetfile cannot be associated with multiple datasets.

Example

add policy dataset ts1 -type IPV4

bind policy dataset

Binds a value of the specified type to the dataset. If the first value is bound by using an index label, the other bind statements to that set should also provide an index. User can bind 50,000 values to a dataset. With the pattern set file, only 10,000 values can be bound. If the dataset is used in a streaming case, then only 5,000 values can be bound to that dataset. A dataset is used in a streaming case when it is used an HTTP body expression, a TCP payload expression, or the rewrite action search parameter. NOTE: With smaller number of values, user can see better performance at the configuration time.

Synopsis

bind policy dataset <name> <value>

Arguments

name Name of the dataset to which to bind the value.

value Value of the specified type that is associated with the dataset. For ipv4 and ipv6, value can be a subnet using the slash notation address/n, where address is the beginning of the subnet and n is the number of left-most bits set in the subnet mask, defining the end of the subnet. The start address will be masked by the subnet mask if necessary, for example for 192.128.128.0/10, the start address will be 192.128.0.0.

index The Index of the value associated with set. Minimum value: 1 Maximum value: 4294967290

endRange The dataset entry is a range from <value> through <end_range>, inclusive. endRange cannot be used if value is an ipv4 or ipv6 subnet and endRange cannot itself be a subnet.

comment Any comments to preserve information about this dataset or a data bound to this dataset.

Example

bind policy dataset ts1 192.168.20.1 -index 2

unbind policy dataset

Unbind string(s) from a dataset.

Synopsis

unbind policy dataset <name> <value>

Arguments

name Name of the dataset from which to unbind the value.

value Value to unbind from the dataset.

endRange End value for a range to unbind. This is optional; just the start range value is sufficient to unbind a range. If specified, it must match the end range specified in the bind. It cannot be a subnet or used with a bound subnet.

Example

unbind policy dataset pat1 bar xyz

policy-evaluation

The following operations can be performed on "policy-evaluation":

show policy evaluation

Executes pixl expression or action and gives result. Result type can be zero or more of: -Bool -Num -Double -Unsigned long -String

Synopsis

show policy evaluation (-expression <expression> | -action <string>) -type <type> -input <string>

Arguments

expression Expression string. For example: http.req.body(100).contains("this").

action Rewrite action name. Supported rewrite action types are: -delete -delete_all -delete_http_header -insert_after -insert_after_all -insert_before -insert_before_all -insert_http_header -replace -replace_all

type Indicates request or response input packet

Possible values: HTTP_REQ, HTTP_RES, TEXT

input Text representation of input packet.

Output

stateflag pitModifiedInputData Text representation of packet after evaluating expression or rewrite action.

pitBoolResult Result of the expression in bool format.

pitNumResult Result of the expression in num format.

pitDoubleResult Result of the expression in double format.

pitUlongResult Result of the expression in unsigned long format.

pitRefResult Result of the expression in string format.

isPitEmptyRefResult Result of the expression is empty string.

pitOffsetResult Offset of the resultant sting.

pitOffsetResultLen Offset length of the resultant sting.

isTruncatedRefResult Identify whether ref result is truncated result.

pitBoolEvalTime Average evaluation time of bool type expression in nanoseconds.

pitNumEvalTime Average evaluation time of num type expression in nanoseconds.

pitDoubleEvalTime Average evaluation time of double type expression in nanoseconds.

pitUlongEvalTime Average evaluation time of unsigned long type expression in nanoseconds.

pitRefEvalTime Average evaluation time of string type expression in nanoseconds.

pitOffsetEvalTime Average evaluation time in finding offset of the resultant string in the input. Time is in nanoseconds.

pitActionEvalTime Average evaluation time of rewrite action in nanoseconds.

pitOperationPerformerArray Details of the operation Citrix ADC performed at various offsets during applying of rewrite action on input data. Operation can be insertion, modfication or deletion.

pitOldOffsetArray Details of the offsets in the input data at which Citrix ADC either inserted or modified or deleted data during applying of rewrite action.

pitNewOffsetArray Details of the offsets in the output data at which Citrix ADC either inserted or modified or deleted data during applying of rewrite action.

pitOffsetLengthArray Details of the lengths of the data which Citrix ADC modified or deleted during applying of rewrite action.

pitOffsetNewLengthArray Details of the lengths of the data which Citrix ADC either inserted or modified during applying of rewrite action.

pitBoolErrorResult Result of the bool type expression if any error occurs during evaluation. Result will be in string format.

pitNumErrorResult Result of the num type expression if any error occurs during evaluation. Result will be in string format.

pitDoubleErrorResult Result of the double type expression if any error occurs during evaluation. Result will be in string format.

pitUlongErrorResult Result of the unsigned long type expression if any error occurs during evaluation. Result will be in string format.

pitRefErrorResult Result of the ref type expression if any error occurs during evaluation. Result will be in string format.

pitOffsetErrorResult Result of the expression if any error occurs in calculating offset. Result will be in string format.

pitActionErrorResult Result of the action if any error occurs in evaluation. Result will be in string format.

devno count

Example

Example 1: show policy evaluation -action rw_act_1 -type http_req -input 'GET / HTTP/1.1\\r\\nHost: abc.com\\r\\n\\r\\n' Example 2: show policy evaluation -expression 'http.res.body(10).contains("foo")' -type http_res -input "HTTP/1.1 200 OK\\r\\n\\r\\nabcdfooabcd" Example 3: show policy evaluation -expression 'text.contains("foo")' -type text -input "testing_test_foo"

policy-expression

The following operations can be performed on "policy-expression":

unset| set| add| show| rm|

unset policy expression

Use this command to remove policy expression settings.Refer to the set policy expression command for meanings of the arguments.

Synopsis

unset policy expression <name>

set policy expression

Modifies the attributes of a named policy expression.

Synopsis

set policy expression <name>

Arguments

name Name of the policy expression to be modified.

value The expression string.

comment Any comments associated with the expression. Displayed upon viewing the policy expression.

clientSecurityMessage The client security message that will be displayed on failure of this expression. Only relevant for end point check expressions.

add policy expression

Creates a classic or default syntax named expression, which can be used in multiple policies. For example, you can create the following named expressions, ExpressionA and ExpressionB: ExpressionA: http.req.body(100).contains("A") ExpressionB: http.req.body(100).contains("B")

You could then create an expression of the form:

Synopsis

add policy expression <name> <value>

Arguments

name Unique name for the expression. Not case sensitive. Must begin with an ASCII letter or underscore (_) character, and must consist only of ASCII alphanumeric or underscore characters. Must not begin with 're' or 'xp' or be a word reserved for use as an expression qualifier prefix (such as HTTP) or enumeration value (such as ASCII). Must not be the name of an existing named expression, pattern set, dataset, stringmap, or HTTP callout.

value Expression string. For example: http.req.body(100).contains("this").

comment Any comments associated with the expression. Displayed upon viewing the policy expression.

clientSecurityMessage Message to display if the expression fails. Allowed for classic end-point check expressions only.

show policy expression

Displays information about the available named policy expressions.

Synopsis

show policy expression

Arguments

name Name of the policy expression to display. If a name is not provided, information about all policy expressions is shown.

type Type of expression. Can be a classic or default syntax (advanced) expression.

Possible values: CLASSIC, ADVANCED

Output

value The expression string.

hits The total number of hits.

piHits The total number of hits.

type The type of expression. This is for output only.

clientSecurityMessage The client security message that will be displayed on failure of the client security check.

comment Any comments associated with the expression. Displayed upon viewing the policy expression.

stateflag flag isDefault A value of true is returned if it is a default policy expression.

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

gslbBindings Number of times expression is being used in the GSLB config.

devno count

rm policy expression

Removes a named policy expression. If the expression is used by a policy or filter, you must remove the policy or filter before removing the expression.

Synopsis

rm policy expression <name> ...

Arguments

name Name of the policy expression to be removed.

policy-httpCallout

The following operations can be performed on "policy-httpCallout":

rm| add| show| unset| set|

rm policy httpCallout

Removes an HTTP callout. You cannot remove an HTTP callout that is used in any part of policy, action, or expression.

Synopsis

rm policy httpCallout <name>

Arguments

name Name of the HTTP callout to remove.

Example

rm policy httpcallout h1

add policy httpCallout

Adds an expression element that, when evaluated, sends an HTTP request to a specified service and receives an HTTP response from the service. Can be used to obtain additional information for use in evaluating policy rules and other expressions. The expression prefix SYS.HTTP_CALLOUT invokes an HTTP callout. You can construct the HTTP callout request in one of two ways:

- Specify individual parts of the request by using the HTTP method, host expression, URL stem expression, and header parameters. These parts are evaluated at run time and concatenated to build the request.
- Specify the entire HTTP request in a single expression.

Synopsis

add policy httpCallout <name>

Arguments

name Name for the HTTP callout. Not case sensitive. Must begin with an ASCII letter or underscore (_) character, and must consist only of ASCII alphanumeric or underscore characters. Must not begin with 're' or 'xp' or be a word reserved for use as an expression qualifier prefix (such

as HTTP) or enumeration value (such as ASCII). Must not be the name of an existing named expression, pattern set, dataset, stringmap, or HTTP callout.

IPAddress IP Address of the server (callout agent) to which the callout is sent. Can be an IPv4 or IPv6 address. Mutually exclusive with the Virtual Server parameter. Therefore, you cannot set the <IP Address, Port> and the Virtual Server in the same HTTP callout.

port Server port to which the HTTP callout agent is mapped. Mutually exclusive with the Virtual Server parameter. Therefore, you cannot set the <IP Address, Port> and the Virtual Server in the same HTTP callout. Minimum value: 1

vServer Name of the load balancing, content switching, or cache redirection virtual server (the callout agent) to which the HTTP callout is sent. The service type of the virtual server must be HTTP. Mutually exclusive with the IP address and port parameters. Therefore, you cannot set the <IP Address, Port> and the Virtual Server in the same HTTP callout.

returnType Type of data that the target callout agent returns in response to the callout. Available settings function as follows:

- TEXT - Treat the returned value as a text string.
- NUM - Treat the returned value as a number.
- BOOL - Treat the returned value as a Boolean value. Note: You cannot change the return type after it is set.

Possible values: BOOL, NUM, TEXT

httpMethod Method used in the HTTP request that this callout sends. Mutually exclusive with the full HTTP request expression.

Possible values: GET, POST

hostExpr String expression to configure the Host header. Can contain a literal value (for example, 10.101.10.11) or a derived value (for example, http.req.header("Host")). The literal value can be an IP address or a fully qualified domain name. Mutually exclusive with the full HTTP request expression.

urlStemExpr String expression for generating the URL stem. Can contain a literal string (for example, "/mysite/index.html") or an expression that derives the value (for example, http.req.url). Mutually exclusive with the full HTTP request expression.

headers One or more headers to insert into the HTTP request. Each header is specified as "name(expr)", where expr is an expression that is evaluated at runtime to provide the value for the named header. You can configure a maximum of eight headers for an HTTP callout. Mutually exclusive with the full HTTP request expression.

parameters One or more query parameters to insert into the HTTP request URL (for a GET request) or into the request body (for a POST request). Each parameter is specified as "name(expr)", where expr is an expression that is evaluated at run time to provide the value for the named parameter (name=value). The parameter values are URL encoded. Mutually exclusive with the full HTTP request expression.

bodyExpr An advanced string expression for generating the body of the request. The expression can contain a literal string or an expression that derives the value (for example, client.ip.src). Mutually exclusive with -fullReqExpr.

fullReqExpr Exact HTTP request, in the form of an expression, which the Citrix ADC sends to the callout agent. If you set this parameter, you must not include HTTP method, host expression, URL stem expression, headers, or parameters. The request expression is constrained by the feature for which the callout is used. For example, an HTTP.RES expression cannot be used in a request-time policy bank or in a TCP content switching policy bank. The Citrix ADC does not check the validity of this request. You must manually validate the request.

scheme Type of scheme for the callout server.

Possible values: http, https

resultExpr Expression that extracts the callout results from the response sent by the HTTP callout agent. Must be a response based expression, that is, it must begin with HTTP.RES. The operations in this expression must match the return type. For example, if you configure a return type of TEXT, the result expression must be a text based expression. If the return type is NUM, the result expression (resultExpr) must return a numeric value, as in the following example: http.res.body(10000).length.

cacheForSecs Duration, in seconds, for which the callout response is cached. The cached responses are stored in an integrated caching content group named "calloutContentGroup". If no duration is configured, the callout responses will not be cached unless normal caching configuration is used to cache them. This parameter takes precedence over any normal caching configuration that would otherwise apply to these responses. Note that the calloutContentGroup definition may not be modified or removed nor may it be used with other cache policies. Minimum value: 1 Maximum value: 31536000

comment Any comments to preserve information about this HTTP callout.

Example

add policy httpcallout h1 -IPAddress 1.1.1.1 -PORT 80

show policy httpCallout

Displays information about the configured HTTP callouts.

Synopsis

show policy httpCallout

Arguments

name Name of the HTTP callout to display. If a name is not provided, information about all configured HTTP callouts is shown.

Output

stateflag IPAddress Server IP address.

port Server port.

vServer Vserver name

returnType Return type of the http callout

scheme Type of scheme(HTTP/HTTPS) for the callout server

httpMethod Http callout request type

hostExpr PI string expression for Host

urlStemExpr PI string expression for URL stem

headers PI string expression for request http headers

parameters PI string expression for request query parameters

fullReqExpr PI string expression for full http callout request

resultExpr PI string expression for http callout response

hits Total hits

undefHits Total undefs

svrState The state of the service

effectiveState The effective state of the service

undefReason Reason for last undef

recursiveCallout Number of recursive callouts

bodyExpr An advanced string expression for generating the body of the request. The expression can contain a literal string or an expression that derives the value (for example, client.ip.src). Mutually exclusive with -fullReqExpr.

cacheForSecs Duration, in seconds, for which the callout response is cached. The cached responses are stored in an integrated caching content group named "calloutContentGroup". If no duration is configured, the callout responses will not be cached unless normal caching configuration is used to cache them. This parameter takes precedence over any normal caching configuration that would otherwise apply to these responses. Note that the calloutContentGroup definition may not be modified or removed nor may it be used with other cache policies.

comment Any comments to preserve information about this HTTP callout.

gslbBindings Number of times expression is being used in the GSLB config.

devno count

Example

show policy httpcallout h1

unset policy httpCallout

Use this command to remove policy httpCallout settings.Refer to the set policy httpCallout command for meanings of the arguments.

Synopsis

unset policy httpCallout <name>

set policy httpCallout

Modifies the attributes of an existing HTTP callout element.

Synopsis

set policy httpCallout <name>

Arguments

name Name of the HTTP callout to configure.

IPAddress IP Address of the server (callout agent) to which the callout is sent. Can be an IPv4 or IPv6 address. Mutually exclusive with the Virtual Server parameter. Therefore, you cannot set the <IP Address, Port> and the Virtual Server in the same HTTP callout.

port Server port to which the HTTP callout agent is mapped. Mutually exclusive with the Virtual Server parameter. Therefore, you cannot set the <IP Address, Port> and the Virtual Server in the same HTTP callout. Minimum value: 1

vServer Name of the load balancing, content switching, or cache redirection virtual server (the callout agent) to which the HTTP callout is sent. The service type of the virtual server must be HTTP. Mutually exclusive with the IP address and port parameters. Therefore, you cannot set the <IP Address, Port> and the Virtual Server in the same HTTP callout.

returnType Type of data that the target callout agent returns in response to the callout. Available settings function as follows:

- TEXT - Treat the returned value as a text string.
- NUM - Treat the returned value as a number.
- BOOL - Treat the returned value as a Boolean value. Note: You cannot change the return type after it is set.

Possible values: BOOL, NUM, TEXT

httpMethod Method used in the HTTP request that this callout sends. Mutually exclusive with the full HTTP request expression.

Possible values: GET, POST

hostExpr String expression to configure the Host header. Can contain a literal value (for example, 10.101.10.11) or a derived value (for example, http.req.header("Host")). The literal value can be an IP address or a fully qualified domain name. Mutually exclusive with the full HTTP request expression.

urlStemExpr String expression for generating the URL stem. Can contain a literal string (for example, "/mysite/index.html") or an expression that derives the value (for example, http.req.url). Mutually exclusive with the full HTTP request expression.

headers One or more headers to insert into the HTTP request. Each header is specified as "name(expr)", where expr is an expression that is evaluated at runtime to provide the value for the named header. You can configure a maximum of eight headers for an HTTP callout. Mutually exclusive with the full HTTP request expression.

parameters One or more query parameters to insert into the HTTP request URL (for a GET request) or into the request body (for a POST request). Each parameter is specified as "name(expr)", where expr is an expression that is evaluated at run time to provide the value for the named parameter (name=value). The parameter values are URL encoded. Mutually exclusive with the full HTTP request expression.

bodyExpr An advanced string expression for generating the body of the request. The expression can contain a literal string or an expression that derives the value (for example, client.ip.src). Mutually exclusive with -fullReqExpr.

fullReqExpr Exact HTTP request, in the form of an expression, which the Citrix ADC sends to the callout agent. If you set this parameter, you must not include HTTP method, host expression, URL stem expression, headers, or parameters. The request expression is constrained by the feature for which the callout is used. For example, an HTTP.RES expression cannot be used in a request-time policy bank or in a TCP content switching policy bank. The Citrix ADC does not check the validity of this request. You must manually validate the request.

scheme Type of scheme for the callout server.

Possible values: http, https

resultExpr Expression that extracts the callout results from the response sent by the HTTP callout agent. Must be a response based expression, that is, it must begin with HTTP.RES. The operations in this expression must match the return type. For example, if you configure a return type of TEXT, the result expression must be a text based expression. If the return type is NUM, the result expression (resultExpr) must return a numeric value, as in the following example: http.res.body(10000).length.

cacheForSecs Duration, in seconds, for which the callout response is cached. The cached responses are stored in an integrated caching content group named "calloutContentGroup". If no duration is configured, the callout responses will not be cached unless normal caching configuration is used to cache them. This parameter takes precedence over any normal caching configuration that would otherwise apply to these responses. Note that the calloutContentGroup definition may not be modified or removed nor may it be used with other cache policies. Minimum value: 1 Maximum value: 31536000

comment Any comments to preserve information about this HTTP callout.

Example

set policy httpcallout h1 -IPAddress 1.1.1.1 -PORT 80

policy-map

The following operations can be performed on "policy-map":

add| show| rm|

add policy map

Creates a policy to map a publicly known domain name to a target domain name for a reverse proxy virtual server used by the cache redirection feature. Optionally, you can also specify a source and target URL. The map policy can be associated with a reverse proxy cache redirection virtual server by using the 'bind cr vserver' command. There can be only one default map policy for a domain.

Synopsis

add policy map <mapPolicyName> -sd <string>

Arguments

mapPolicyName Name for the map policy. Must begin with a letter, number, or the underscore (*) character and must consist only of letters, numbers, and the hash (#), period (.), colon (:), space ( ), at (@), equals (=), hyphen (-), and underscore (*) characters.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my map" or 'my map').

sd Publicly known source domain name. This is the domain name with which a client request arrives at a reverse proxy virtual server for cache redirection. If you specify a source domain, you must specify a target domain.

su Source URL. Specify all or part of the source URL, in the following format: /[ ] .

td Target domain name sent to the server. The source domain name is replaced with this domain name.

tu Target URL. Specify the target URL in the following format: /[prefix] [*].

Example

Example 1 The following example creates a default map policy (map1) for the source domain www.a.com. Any client requests with this source domain in the host header is changed to www.real_a.com. add policy map map2 -sd www.a.com -td www.real.a.com Example 2 This example shows how to create a URL map policy (map2) if you want to translate /sports.html in the incoming request to /news.html in addition to mapping the source domain www.a.com to www.real_a.com in the outgoing request. add policy map map2 -sd www.a.com -td www.real_a.com -su /sports.html -tu /news.html These type of map policies, called "URL map policies," have the following restrictions: lURL map policies belonging to www.a.com cannot be added without first adding a default map policy as described in Example 1. lIf a source suffix has been specified for URL map policy, a destination suffix must also be specified. lIf an exact URL has been specified as the source, then the target URL should also be exact URL. lIf there is a source prefix in the URL, there must be also a destination prefix in the URL.

show policy map

Displays information about the available policy maps.

Synopsis

show policy map

Arguments

mapPolicyName Name of the policy map to display. If a name is not provided, information of all configured policy maps is shown.

Output

sd Publicly known source domain name. This is the domain name with which a client request arrives at a reverse proxy virtual server for cache redirection. If you specify a source domain, you must specify a target domain.

su The source URL.

td The domain name sent to the server.

tu The target URL.

targetName The expression string.

devno count stateflag

rm policy map

Removes a map policy. Before removing the map policy, you must unbind the map policy from the reverse proxy virtual server.

Synopsis

rm policy map <mapPolicyName>

Arguments

mapPolicyName Name of the policy map to remove.

policy-param

The following operations can be performed on "policy-param":

unset| set| show|

unset policy param

Use this command to remove policy param settings.Refer to the set policy param command for meanings of the arguments.

Synopsis

unset policy param -timeout

set policy param

Sets the given Policy parameter(s).

Synopsis

set policy param -timeout <msecs>

Arguments

timeout Maximum time in milliseconds to allow for processing expressions and policies without interruption. If the timeout is reached then the evaluation causes an UNDEF to be raised and no further processing is performed. Default value: 3900 Minimum value: 1 Maximum value: 5000

Example

set policy param -timeout 5

show policy param

Displays the policy parameters.

Synopsis

show policy param

Arguments

Output

timeout Execution timeout.

Example

show policy param

policy-patset

The following operations can be performed on "policy-patset":

rm| show| bind| add| unbind|

rm policy patset

Removes a pattern set. If the pattern set is used by an expression in another object, such as a policy, you must remove the object before removing the pattern set.

Synopsis

rm policy patset <name>

Arguments

name Name of the pattern set to remove.

Example

rm policy patset pat1

show policy patset

Displays the list of pattern sets configured on the appliance.

Synopsis

show policy patset

Arguments

name Name of the pattern set for which to display the detailed information. If a name is not provided, a list of all pattern sets configured on the appliance is shown.

Output

stateflag string String of characters that constitutes a pattern. For more information about the characters that can be used, refer to the character set parameter. Note: Minimum length for pattern sets used in rewrite actions of type REPLACE_ALL, DELETE_ALL, INSERT_AFTER_ALL, and INSERT_BEFORE_ALL, is three characters.

index The index of the string associated with the patset.

charset Character set associated with the characters in the string. Note: UTF-8 characters can be entered directly (if the UI supports it) or can be encoded as a sequence of hexadecimal bytes '\xNN'. For example, the UTF-8 character 'ü' can be encoded as '\xC3\xBC'.

isDefault builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

MaxIndex Maximum number of patterns bounded to pattern set. The maxindex value will not be decreased when we unbind a pattern from the patset. This field is used in auto-generated indexing type.

comment Any comments to preserve information about this patset or a pattern bound to this patset.

patsetFile File which contains list of patterns that needs to be bound to the patset. A patsetfile cannot be associated with multiple patsets.

devno count

Example

show policy patset pat1

bind policy patset

Binds a string to a pattern set. User can bind 50,000 patterns to a pattern set. With the pattern set file, only 10,000 patterns can be bound. If the pattern set is used in a streaming case, then only 5,000 patterns can be bound to that pattern set. A pattern set is used in a streaming case when it is used in an HTTP body expression, a TCP payload expression, or the rewrite action search parameter. NOTE: With smaller number of patterns, user can see better performance at the configuration time.

Synopsis

bind policy patset <name> <string>

Arguments

name Name of the pattern set to which to bind the string.

string String of characters that constitutes a pattern. For more information about the characters that can be used, refer to the character set parameter. Note: Minimum length for pattern sets used in rewrite actions of type REPLACE_ALL, DELETE_ALL, INSERT_AFTER_ALL, and INSERT_BEFORE_ALL, is three characters.

index Integer that identifies the string pattern within the pattern set. You can assign index values or allow them to be assigned automatically. If you specify an index for the first pattern that you bind to the set, you must do so for each subsequent pattern. If you do not specify an index for the first pattern, the Citrix ADC generates an index. If you subsequently specify an index when binding a pattern to the set, an error message appears. The pattern index of a matching pattern can be used within expressions. For example, HTTP.REQ.URL.EQUALS_INDEX("test_url").EQ(5), returns true if the request URL matches the strings in the test_url pattern set with index 5. Minimum value: 1 Maximum value: 4294967290

charset Character set associated with the characters in the string. Note: UTF-8 characters can be entered directly (if the UI supports it) or can be encoded as a sequence of hexadecimal bytes '\xNN'. For example, the UTF-8 character 'ü' can be encoded as '\xC3\xBC'.

Possible values: ASCII, UTF_8

comment Any comments to preserve information about this patset or a pattern bound to this patset.

Example

bind policy patset pat1 bar -index 2

add policy patset

Adds a pattern set. A pattern set contains a name and one or more string patterns. Pattern sets can be used in expressions to match a set of strings. For example, HTTP.REQ.URL.EQUALS_ANY("test_urls"), where test_urls is a pattern set containing URL strings. Pattern sets can also be used in the search parameter of a rewrite action. Each string pattern is assigned an index that enables you to select the associated string from the set. The patset file option can be used to bind the patterns contained in a file, which is imported from Citrix ADC or from an external location (please check import/add/update patsetfile). A patset can be configured with at most one patsetfile

Synopsis

add policy patset <name>

Arguments

name Unique name of the pattern set. Not case sensitive. Must begin with an ASCII letter or underscore (_) character and must contain only alphanumeric and underscore characters. Must not be the name of an existing named expression, pattern set, dataset, string map, or HTTP callout.

comment Any comments to preserve information about this patset or a pattern bound to this patset.

patsetFile File which contains list of patterns that needs to be bound to the patset. A patsetfile cannot be associated with multiple patsets.

Example

add policy patset pat1

unbind policy patset

Unbinds a string from a pattern set.

Synopsis

unbind policy patset <name> <string> ...

Arguments

name Name of the pattern set from which to unbind a string.

string String of characters to unbind from the pattern set.

Example

unbind policy patset pat1 bar xyz

policy-patsetFile

The following operations can be performed on "policy-patsetFile":

rm| add| update| show| import|

rm policy patsetFile

Deletes the specified patset file.

Synopsis

rm policy patsetFile <name>

Arguments

name Name to assign to the imported patset file. Unique name of the pattern set. Not case sensitive. Must begin with an ASCII letter or underscore (_) character and must contain only alphanumeric and underscore characters.

Example

rm policy patsetfile patsetfile1

add policy patsetFile

Loads the patterns from the specified patset file.

Synopsis

add policy patsetFile <name>

Arguments

name Name to assign to the imported patset file. Unique name of the pattern set. Not case sensitive. Must begin with an ASCII letter or underscore (_) character and must contain only alphanumeric and underscore characters.

comment Any comments to preserve information about this patsetfile.

Example

add policy patsetfile patsetfile1

update policy patsetFile

Loads an updated pattern set from specified patset file.

Synopsis

update policy patsetFile <name>

Arguments

name Name to assign to the imported patset file. Unique name of the pattern set. Not case sensitive. Must begin with an ASCII letter or underscore (_) character and must contain only alphanumeric and underscore characters.

Example

update policy patsetfile patsetfile1

show policy patsetFile

Displays a list of all the imported patset files on the Citrix ADC.

Synopsis

show policy patsetFile

Arguments

name Name to assign to the imported patset file. Unique name of the pattern set. Not case sensitive. Must begin with an ASCII letter or underscore (_) character and must contain only alphanumeric and underscore characters.

imported When set, display only shows all imported patsetfiles. Default value: 0

Output

src URL in protocol, host, path, and file name format from where the patset file will be imported. If file is already present, then it can be imported using local keyword (import patsetfile local:filename patsetfile1) NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access

delimiter patset file patterns delimiter.

charset Character set associated with the characters in the string.

totalPatterns Total number of patterns in the patset file.

boundPatterns Total number of patterns bound to a patset.

patsetName The patset with which the patsetfile is associated.

comment Any comments to preserve information about this patsetfile.

bindStatusCode The status code of pattern bindings to patset.

bindStatus The status of pattern bindings to patset.

devno count stateflag

Example

show policy patsetfile

import policy patsetFile

Import a patset file to the Citrix ADC and assign it a name.

Synopsis

import policy patsetFile <src> <name>

Arguments

src URL in protocol, host, path, and file name format from where the patset file will be imported. If file is already present, then it can be imported using local keyword (import patsetfile local:filename patsetfile1) NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access

name Name to assign to the imported patset file. Unique name of the pattern set. Not case sensitive. Must begin with an ASCII letter or underscore (_) character and must contain only alphanumeric and underscore characters.

overwrite Overwrites the existing file

delimiter patset file patterns delimiter. Default value: 10

charset Character set associated with the characters in the string.

Possible values: ASCII, UTF_8

Example

import policy patsetfile http://www.example.com/patterns patsetfile1

policy-stringmap

The following operations can be performed on "policy-stringmap":

unset| show| set| add| unbind| rm| bind|

unset policy stringmap

Use this command to remove policy stringmap settings.Refer to the set policy stringmap command for meanings of the arguments.

Synopsis

unset policy stringmap <name> -comment

show policy stringmap

Displays a list of available string maps.

Synopsis

show policy stringmap

Arguments

name Name of the string map to display. If a name is not provided, a list of all the configured string maps is shown.

Output

stateflag comment Comments associated with the string map or key-value pair bound to this string map.

key Character string constituting the key to be bound to the string map. The key is matched against the data processed by the operation that uses the string map. The default character set is ASCII. UTF-8 characters can be included if the character set is UTF-8. UTF-8 characters can be entered directly (if the UI supports it) or can be encoded as a sequence of hexadecimal bytes '\xNN'. For example, the UTF-8 character 'ü' can be encoded as '\xC3\xBC'.

value Character string constituting the value associated with the key. This value is returned when processed data matches the associated key. Refer to the key parameter for details of the value character set.

devno count

Example

show stringmap custom_stringmap . Displays all the key-value pairs of a string map whose name is custom-stringmap

set policy stringmap

Modifies the attributes of an existing string map.

Synopsis

set policy stringmap <name> -comment <string>

Arguments

name Name of the string map to be modified.

comment Comments associated with the string map or key-value pair bound to this string map.

Example

i)set stringmap custom_stringmap -comment "custom string map is for URLs." .This updates the comment associated with the string map whose name is custom_stringmap

add policy stringmap

Creates a string map. You must use the 'bind policy stringmap' command to bind strings to this string map.

Synopsis

add policy stringmap <name>

Arguments

name Unique name for the string map. Not case sensitive. Must begin with an ASCII letter or underscore (_) character, and must consist only of ASCII alphanumeric or underscore characters. Must not begin with 're' or 'xp' or be a word reserved for use as an expression qualifier prefix (such as HTTP) or enumeration value (such as ASCII). Must not be the name of an existing named expression, pattern set, dataset, string map, or HTTP callout.

comment Comments associated with the string map or key-value pair bound to this string map.

Example

i)add stringmap custom_stringmap .This creates a new string map with name custom_stringmap.

unbind policy stringmap

Removes a key from the string map.

Synopsis

unbind policy stringmap <name> <key>

Arguments

name Name of the string map from which to remove a key.

key Key to remove from the string map.

Example

unbind stringmap custom_stringmap key1 .This removes the key "key1" and its associated value from the string map whose name is custom_stringmap.

rm policy stringmap

Removes a string map. String maps can be removed only if not used in any part of policy, action, or expression.

Synopsis

rm policy stringmap <name>

Arguments

name Name of the string map to remove.

Example

i)rm stringmap custom_stringmap .This removes a string map whose name is custom_stringmap

bind policy stringmap

Binds a key and its associated value to a string map. If the key already exists and has a different value, the old value is overwritten with the new value.

Synopsis

bind policy stringmap <name> <key> <value>

Arguments

name Name of the string map to which to bind the key-value pair.

key Character string constituting the key to be bound to the string map. The key is matched against the data processed by the operation that uses the string map. The default character set is ASCII. UTF-8 characters can be included if the character set is UTF-8. UTF-8 characters can be entered directly (if the UI supports it) or can be encoded as a sequence of hexadecimal bytes '\xNN'. For example, the UTF-8 character 'ü' can be encoded as '\xC3\xBC'.

value Character string constituting the value associated with the key. This value is returned when processed data matches the associated key. Refer to the key parameter for details of the value character set.

comment Comments associated with the string map or key-value pair bound to this string map.

Example

bind stringmap custom_stringmap "key-string" "value-string" .This adds the key "key-string" and its associated value "value-string" to the string map whose name is custom_stringmap.

policy-urlset

The following operations can be performed on "policy-urlset":

add| rm| import| show| update| export|

add policy urlset

Adds a url set.

Synopsis

add policy urlset <name>

Arguments

name Unique name of the url set. Not case sensitive. Must begin with an ASCII letter or underscore (_) character and must contain only alphanumeric and underscore characters. Must not be the name of an existing named expression, pattern set, dataset, string map, or HTTP callout.

comment Any comments to preserve information about this url set.

Example

add policy urlset urlset1

rm policy urlset

Removes a url set. If the url set is used by an expression in another object, such as a policy, you must remove the object before removing the url set.

Synopsis

rm policy urlset <name>

Arguments

name Name of the url set to remove.

Example

rm urlset urlset1

import policy urlset

Imports the specified urlset to the Citrix ADC, assigns it the specified name.

Synopsis

import policy urlset <name> -url

Arguments

name Unique name of the url set. Not case sensitive. Must begin with an ASCII letter or underscore (_) character and must contain only alphanumeric and underscore characters. Must not be the name of an existing named expression, pattern set, dataset, string map, or HTTP callout.

overwrite Overwrites the existing file. Default value: 0

delimiter CSV file record delimiter. Default value: 44

rowSeparator CSV file row separator. Default value: 10

url URL (protocol, host, path and file name) from where the CSV (comma separated file) file will be imported or exported. Each record/line will one entry within the urlset. The first field contains the URL pattern, subsequent fields contains the metadata, if available. HTTP, HTTPS and FTP protocols are supported. NOTE: The operation fails if the destination HTTPS server requires client certificate authentication for access.

interval The interval, in seconds, rounded down to the nearest 15 minutes, at which the update of urlset occurs. Default value: 0 Maximum value: 2592000

privateSet Prevent this urlset from being exported. Default value: 0

subdomainExactMatch Force exact subdomain matching, ex. given an entry 'google.com' in the urlset, a request to 'news.google.com' won't match, if subdomainExactMatch is set. Default value: 0

MatchedId An ID that would be sent to AppFlow to indicate which URLSet was the last one that matched the requested URL. Default value: 1 Minimum value: 2 Maximum value: 31

canaryUrl Add this URL to this urlset. Used for testing when contents of urlset is kept confidential.

Example

import policy urlset urlset1 -url http://www.example.com/file_1

show policy urlset

Displays information about the configured urlsets.

Synopsis

show policy urlset

Arguments

name Name of the url set for which to display the detailed information. If a name is not provided, a list of all url sets configured on the appliance is shown.

imported when set, display shows all imported urlsets. Default value: 0

Output

stateflag comment Any comments to preserve information about this url set.

patternCount Number of patterns in this urlset.

url URL (protocol, host, path and file name) from where the CSV (comma separated file) file will be imported or exported. Each record/line will one entry within the urlset. The first field contains the URL pattern, subsequent fields contains the metadata, if available. HTTP, HTTPS and FTP protocols are supported. NOTE: The operation fails if the destination HTTPS server requires client certificate authentication for access.

delimiter CSV file record delimiter.

rowSeparator CSV file row separator.

interval The interval, in seconds, rounded down to the nearest 15 minutes, at which the update of urlset occurs.

MatchedId An ID that would be sent to AppFlow to indicate which URLSet was the last one that matched the requested URL.

canaryUrl Add this URL to this urlset. Used for testing when contents of urlset is kept confidential.

devno count

Example

show policy urlset urlset1

update policy urlset

Update the specified urlset from the source.

Synopsis

update policy urlset <name>

Arguments

name Name of the urlset to update.

Example

update policy urlset urlset1

export policy urlset

Exports the specified urlset to the URL. Ensure the URL accepts a PUT request for HTTP/HTTPS URL.

Synopsis

export policy urlset <name> -url

Arguments

name Unique name of the url set. Not case sensitive. Must begin with an ASCII letter or underscore (_) character and must contain only alphanumeric and underscore characters. Must not be the name of an existing named expression, pattern set, dataset, string map, or HTTP callout.

url URL (protocol, host, path and file name) from where the CSV (comma separated file) file will be imported or exported. Each record/line will one entry within the urlset. The first field contains the URL pattern, subsequent fields contains the metadata, if available. HTTP, HTTPS and FTP protocols are supported. NOTE: The operation fails if the destination HTTPS server requires client certificate authentication for access.

Example

export policy urlset urlset1 -url http://www.example.com/PUT_file_1

protocol

Protocol

The entities on which you can perform NetScaler CLI operations:

- protocol-http
- protocol-http2
- protocol-http3
- protocol-httpBand
- protocol-icmp
- protocol-icmpv6
- protocol-ip
- protocol-ipv6
- protocol-mptcp
- protocol-quic
- protocol-quicbridge
- protocol-tcp
- protocol-udp

protocol-http

The following operations can be performed on "protocol-http":

stat protocol http

Displays statistics of the HTTP protocol.

Synopsis

stat protocol http

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Total requests (HTReqRx) Total number of HTTP requests received.

Total responses (HTRspRx) Total number of HTTP responses sent.

Request bytes received (HTReqbRx) Total number of bytes of HTTP request data received.

Response bytes received (HTRspbRx) Total number of bytes of HTTP response data received.

GETs (HTGETs) Total number of HTTP requests received with the GET method.

POSTs (HTPOSTs) Total number of HTTP requests received with the POST method.

Other methods (HTOthers) Total number of HTTP requests received with methods other than GET and POST. Some of the other well-defined HTTP methods are HEAD, PUT, DELETE, OPTIONS, and TRACE. User-defined methods are also allowed.

HTTP/1.0 requests (HT10ReqRx) Total number of HTTP/1.0 requests received.

HTTP/1.1 requests (HT11ReqRx) Total number of HTTP/1.1 requests received.

Content-length requests (HTCLnReq) Total number of HTTP requests in which the Content-length field of the HTTP header has been set. Content-length specifies the length of the content, in bytes, in the associated HTTP body.

Chunked requests (HTChkReq) Total number of HTTP requests in which the Transfer-Encoding field of the HTTP header has been set to chunked.

Request bytes transmitted (HTReqbTx) Total number of bytes of HTTP request data transmitted.

HTTP/1.0 responses (HT10RspRx) Total number of HTTP/1.0 responses sent.

HTTP/1.1 responses (HT11RspRx) Total number of HTTP/1.1 responses sent.

Content-length responses (HTCLnRsp) Total number of HTTP responses sent in which the Content-length field of the HTTP header has been set. Content-length specifies the length of the content, in bytes, in the associated HTTP body.

Chunked responses (HTChunk) Total number of HTTP responses sent in which the Transfer-Encoding field of the HTTP header has been set to chunked. This setting is used when the server wants to start sending the response before knowing its total length. The server breaks the response into chunks and sends them in sequence, inserting the length of each chunk before the actual data. The message ends with a chunk of size zero.

Multi-part responses (HTMPrtHd) Total number of HTTP multi-part responses sent. In multi-part responses, one or more entities are encapsulated within the body of a single message.

FIN-terminated responses (HTNoCLnChunk) Total number of FIN-terminated responses sent. In FIN-terminated responses, the server finishes sending the data and closes the connection.

Response bytes transmitted (HTRspbTx) Total number of bytes of HTTP response data transmitted.

Incomplete headers (HTIncHd) Total number of HTTP requests and responses received in which the HTTP header spans more than one packet.

Incomplete request headers (HTIncReqHd) Total number of HTTP requests received in which the header spans more than one packet.

Incomplete response headers (HTIncRspHd) Total number of HTTP responses received in which the header spans more than one packet.

HTTP 500 Server-busy Responses (HT500Rsp) Total number of HTTP error responses received. Some of the error responses are: 500 Internal Server Error 501 Not Implemented 502 Bad Gateway 503 Service Unavailable 504 Gateway Timeout 505 HTTP Version Not Supported

Large/Invalid messages (HTInvReq) Total number of requests and responses received with large body.

Large/Invalid chunk requests (HTInvChkRx) Total number of requests received with large chunk size, in which the Transfer-Encoding field of the HTTP header has been set to chunked.

Large/Invalid content-length (HTInvCLn) Total number of requests received with large content, in which the Content-length field of the HTTP header has been set. Content-length specifies the length of the content, in bytes, in the associated HTTP body.

Content-length +TransferEncoding (HTDesynClTe) Total number of requests/responses received with both content-length and transfer encoding headers - RFC7230 Non-compliance

Multiple content-length headers (HTDesynMulCtlen) Total number of request/response received with multiple content-length headers with different values - RFC7230 Non-compliance

Duplicate content-length headers (HTDesynIdenCtlen) Total number of request/response received with duplicate content-length headers - RFC7230 Non-compliance

Invalid host header requests (HTInvalidHostHdr) Total number of request received with invalid host header

Related Commands

- stat protocol http3

protocol-http2

The following operations can be performed on "protocol-http2":

stat protocol http2

Displays statistics of HTTP2 protocol.

Synopsis

stat protocol http2

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

HTTP2 requests (H2ToReq) Total number of http2 requests

HTTP2 responses (H2ToRes) Total number of http2 responses

gRPC requests (GRPCReq) Total number of gRPC requests

gRPC responses (GRPCRes) Total number of gRPC responses

gRPC success (GRPCSuc) Total number of gRPC success

gRPC failures (GRPCFai) Total number of gRPC failures

HTTP2 direct request received (H2ToDir) Total number of http2 direct connections established

HTTP2 server direct (H2SerDi) Number of HTTP/2 server direct

HTTP2 upgrades (H2ReqUpg) Total number of connections upgraded to HTTP2

HTTP2 cipher mismatch (H2NoMatCi) Total number of cipher mismatch failures

HTTP2 server direct failed (H2SerDiFa) Number of HTTP/2 server direct failed

HTTP2 server upgrade failed (H2SerUpFa) Number of HTTP/2 server upgrade failed

HTTP2 request upgrade failed (H2ReqUpFa) Number of HTTP/2 request upgrade failed

HTTP2 DATA frames sent (H2ToDaFrS) Number of HTTP/2 DATA frames sent

HTTP2 HEADER frames sent (H2ToHeFrS) Number of HTTP/2 HEADER frames sent

HTTP2 PRIORITY frames sent (H2ToPrFrS) Number of HTTP/2 PRIORITY frames sent

HTTP2 RST_STREAM frames sent (H2ToRsFrS) Number of HTTP/2 RST_STREAM frames sent

HTTP2 SETTINGS frames sent (H2ToSeFrS) Number of HTTP/2 SETTINGS frames sent

HTTP2 PUSH_PROMISE frames sent (H2ToPPFrS) Number of HTTP/2 PUSH_PROMISE frames sent

HTTP2 PING frames sent (H2ToPiFrS) Number of HTTP/2 PING frames sent

HTTP2 GOAWAY frames sent (H2ToGaFrS) Number of HTTP/2 GOAWAY frames sent

HTTP2 WINDOW_UPDATE frames sent (H2ToWuFrS) Number of HTTP/2 WINDOW_UPDATE frames sent

HTTP2 CONTINUATION frames sent (H2ToCoFrS) Number of HTTP/2 CONTINUATION frames sent

HTTP2 ALTSVC frames sent (H2ToAsFrS) Number of HTTP/2 ALTSVC frames sent

HTTP2 DATA frames rcvd (H2ToDaFrR) Number of HTTP/2 DATA frames received

HTTP2 HEADER frames rcvd (H2ToHeFrR) Total number of http2 header frames received

HTTP2 PRIORITY frames rcvd (H2ToPrFrR) Total number of http2 priority frames received

HTTP2 RST_STREAM Frames rcvd (H2ToRsFrR) Number of HTTP/2 RST_STREAM frames received

HTTP2 SETTING frames rcvd (H2ToSeFrR) Number of HTTP/2 SETTINGS frames received

HTTP2 PUSH_PROMISE Frames rcvd (H2ToPPFrR) Number of HTTP/2 PUSH_PROMISE frames received

HTTP2 Piing Frames rcvd (H2ToPiFrR) Number of HTTP/2 PING frames received

HTTP2 GOAWAY frames rcvd (H2ToGaFrR) Number of HTTP/2 GOAWAY frames received

HTTP2 WINDOW_UPDATE frames rcvd (H2ToWuFrR) Number of HTTP/2 WINDOW_UPDATE frames received

HTTP2 CONTINUATION frames rcvd (H2ToCoFrR) Number of HTTP/2 CONTINUATION frames received

HTTP2 DATA frames (H2InDaFr) Number of HTTP/2 DATA frames

HTTP2 HEADER frames (H2InHeFr) Number of HTTP/2 HEADER frames

HTTP2 PRIORITY frames (H2InPrFr) Number of HTTP/2 PRIORITY frames

HTTP2 RST_STREAM frames (H2InRsFr) Number of HTTP/2 RST_STREAM frames

HTTP2 SETTINGS frames (H2InSeFr) Number of HTTP/2 SETTINGS frames

HTTP2 PUSH_PROMISE frames (H2InPPFr) Number of HTTP/2 PUSH_PROMISE frames

HTTP2 PING frames (H2InPiFr) Number of HTTP/2 PING frames

HTTP2 GOAWAY frames (H2InGaFr) Number of HTTP/2 GOAWAY frames

HTTP2 WINDOW_UPDATE frames (H2InWuFr) Number of HTTP/2 WINDOW_UPDATE frames

HTTP2 CONTINUATION frames (H2InCoFr) Number of HTTP/2 CONTINUATION frames

HTTP2 big frames (H2Fr2Big) Number of HTTP/2 frames received carrying a frame length greater than SETTINGS_MAX_FRAME_SIZE sent by NetScale

PING (H2PinFlo) HTTP/2 number of ping frames received on connection is above rate limit

SETTING (H2SetFlo) HTTP/2 number of settings frames received on connection is above rate limit

RESET (H2ResFlo) HTTP/2 number of reset frames received on connection is above rate limit

EMPTY (H2EmpFlo) HTTP/2 number of empty frames received on connection is above rate limit

Related Commands

- stat protocol http3

protocol-http3

The following operations can be performed on "protocol-http3":

stat protocol http3

Displays statistics of the HTTP3 protocol.

Synopsis

stat protocol http3

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

HTTP3 requests rcvd (H3ReqRcvd) Total number of HTTP/3 requests received

HTTP3 requests sent (H3ReqSent) Total number of HTTP/3 requests sent

HTTP3 responses rcvd (H3ResRcvd) Total number of HTTP/3 responses received

HTTP3 responses sent (H3ResSent) Total number of HTTP/3 responses sent

Connection-info alloc failures (H3ConninfAlcFail) Number of HTTP/3 connection-info allocation failures

NSB alloc failures (H3NSBAlcFail) Number of HTTP/3 NSB allocation failures

Stream-info alloc failures (H3StrminfAlcFail) Number of HTTP/3 stream-info allocation failures

Stream PCB alloc failures (H3StrmPCBAlcFail) Number of HTTP/3 stream PCB allocation failures

Related Commands

- stat protocol quicbridge

protocol-httpBand

The following operations can be performed on "protocol-httpBand":

show| unset| clear| set|

show protocol httpBand

Displays statistics of the HTTP request/response band.

Synopsis

show protocol httpBand -type <type>

Arguments

type Type of statistics to display.

Possible values: REQUEST, RESPONSE, MQTT_JUMBO_REQ

Output

BandRange The range of the HTTP request/response size, in bytes.

numberofbands The total number of http bands.

TotalBandSize The total size of all HTTP requests/responses in this size range.

AvgBandSize The average size of all HTTP requests/responses in this size range.

AvgBandSizeNew The average size of all HTTP requests/responses in this size range.

BandData The total size of all HTTP requests/responses in this size range, expressed as a percentage of the total size of all HTTP requests/responses.

BandDataNew The total size of all HTTP requests/responses in this size range, expressed as a percentage of the total size of all HTTP requests/responses.

AccessCount The number of HTTP requests/responses in this size range.

AccessRatio The number of HTTP requests/responses in this size range, expressed as a percentage of the total number of HTTP requests/responses.

AccessRatioNew The number of HTTP requests/responses in this size range, expressed as a percentage of the total number of HTTP requests/responses.

Totals The total of totalBandSize, avgBandSize, BandData, accessCount, accessRatio respectively.

reqBandSize Band size, in bytes, for HTTP request band statistics. For example, if you specify a band size of 100 bytes, statistics will be maintained and displayed for the following size ranges: 0 - 99 bytes 100 - 199 bytes 200 - 299 bytes and so on.

respBandSize Band size, in bytes, for HTTP response band statistics. For example, if you specify a band size of 100 bytes, statistics will be maintained and displayed for the following size ranges: 0 - 99 bytes 100 - 199 bytes 200 - 299 bytes and so on.

unset protocol httpBand

Use this command to remove protocol httpBand settings.Refer to the set protocol httpBand command for meanings of the arguments.

Synopsis

unset protocol httpBand

clear protocol httpBand

Clears HTTP request/response band statistics.

Synopsis

clear protocol httpBand -type <type>

Arguments

type Type of statistics to display.

Possible values: REQUEST, RESPONSE, MQTT_JUMBO_REQ

Example

clear protocol httpband -type REQUEST, clear protocol httpband -type RESPONSE

set protocol httpBand

Sets the band size for HTTP request/response band statistics.

Synopsis

set protocol httpBand

Arguments

reqBandSize Band size, in bytes, for HTTP request band statistics. For example, if you specify a band size of 100 bytes, statistics will be maintained and displayed for the following size ranges: 0 - 99 bytes 100 - 199 bytes 200 - 299 bytes and so on. Default value: 100 Minimum value: 50

respBandSize Band size, in bytes, for HTTP response band statistics. For example, if you specify a band size of 100 bytes, statistics will be maintained and displayed for the following size ranges: 0 - 99 bytes 100 - 199 bytes 200 - 299 bytes and so on. Default value: 1024 Minimum value: 50

Example

set protocol httpBand -reqBandSize 200 -respBandSize 2048

protocol-icmp

The following operations can be performed on "protocol-icmp":

stat protocol icmp

Displays statistics of the ICMP protocol.

Synopsis

stat protocol icmp

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

ICMP packets received (ICPktRx) ICMP packets received.

ICMP bytes received (ICbRx) Bytes of ICMP data received.

ICMP packets transmitted (ICPktTx) ICMP packets transmitted.

ICMP bytes transmitted (ICbTx) Bytes of ICMP data transmitted.

ICMP echo replies received (ECORepRx) ICMP Ping echo replies received.

ICMP echo replies transmitted (ECORepTx) ICMP Ping echo replies transmitted.

ICMP echos received (ECORx) ICMP Ping Echo Request and Echo Reply packets received.

MTU lookup on dst ip info recvd (MTULkDst) Total number of MTU lookup on destination IP info received on a need fragmentation ICMP error message failed.

ICMP rate threshold (pkts/sec) (ICThs) Limit for ICMP packets handled every 10 milliseconds. Default value, 0, applies no limit. This is a configurable value using the set rateControl command.

ICMP port unreachable received (PortUnRx) ICMP Port Unreachable error messages received. This error is generated when there is no service is running on the port.

ICMP port unreachable generated (PortUnTx) ICMP Port Unreachable error messages generated. This error is generated when there is no service is running on the port.

Need fragmentation received (NeedFrag) ICMP Fragmentation Needed error messages received for packets that need to be fragmented but for which Don't Fragment is specified the header.

ICMP rate threshold exceeded (ICRtEx) Times the ICMP rate threshold is exceeded. If this counter continuously increases, first make sure the ICMP packets received are genuine. If they are, increase the current rate threshold.

ICMP packets dropped (ICPktDr) ICMP packets dropped because the rate threshold has been exceeded.

Bad ICMP checksum (BadCkSum) ICMP Fragmentation Needed error messages received with an ICMP checksum error.

PMTU non-first IP fragments (PMTUerr) ICMP Fragmentation Needed error messages received that were generated by an IP fragment other than the first one.

PMTU Invalid body len received (IvBdyLen) ICMP Fragmentation Needed error messages received that specified an invalid body length.

PMTU no tcp connection (NoTcpCon) ICMP Need Fragmentation error messages received for TCP packets. The state of the connection for these packets is not maintained on the Citrix ADC.

PMTU no udp conection (NoUdpCon) ICMP Need Fragmentation error messages received for UDP packets. The state of the connection for these packets is not maintained on the Citrix ADC.

PMTU invalid tcp seqno recvd (InvSeqNo) ICMP Fragmentation Needed error messages received for packets that contain an invalid TCP address.

Invalid next MTU value recvd (IvNxtMTU) ICMP Fragmentation Needed error messages received in which the Maximum Transmission Unit (MTU) for the next hop is out of range. The range for the MTU is 576-1500.

Next MTU > Current MTU (BigNxMTU) ICMP Fragmentation Needed error messages received in which the value for the next MTU is higher than that of the current MTU.

PMTU Invalid protocol recvd (IvPrtRx) ICMP Fragmentation Needed error messages received that contain a protocol other than TCP and UDP.

PMTU IP check sum error (CkSumErr) ICMP Fragmentation Needed error messages received with an IP checksum error.

PMTU pcb with no link (NoLnkErr) ICMP Fragmentation Needed error messages received on a Protocol Control Block (PCB) with no link. The PCB maintains the state of the connection.

PMTU Discovery not enabled (PMTUdis) ICMP Need Fragmentation error messages received when the PMTU Discovery mode is not enabled.

Related Commands

- stat protocol http3

protocol-icmpv6

The following operations can be performed on "protocol-icmpv6":

stat protocol icmpv6

Displays statistics of the ICMPv6 protocol.

Synopsis

stat protocol icmpv6

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

ICMPv6 packets received (icmpv6RxPkts) ICMPv6 packets received.

ICMPv6 bytes received (icmpv6RxBytes) Bytes of ICMPv6 data received.

ICMPv6 packets transmitted (icmpv6TxPkts) ICMPv6 packets transmitted.

ICMPv6 bytes transmitted (icmpv6TxBytes) Bytes of ICMPv6 data transmitted.

ICMPv6 NA packets received (icmpv6RxNa) ICMPv6 neighbor advertisement packets received. These packets are received in response to a neighbor solicitation message sent out by this node, or if the link layer address of a neighbor has changed.

ICMPv6 NS packets received (icmpv6RxNs) ICMPv6 neighbor solicitation packets received. These packets are received if the link layer address of a neighbor has changed, or in response to a neighbor solicitation message sent out by this node.

ICMPv6 RA packets received (icmpv6RxRa) ICMPv6 router advertisement packets received. These are received at defined intervals or in response to a router solicitation message.

ICMPv6 RS packets received (icmpv6RxRs) ICMPv6 router solicitation packets received. These could be sent by a neighboring router to initiate address resolution.

ICMPv6 Echo Request packets received (icmpv6RxEchoReq) ICMPv6 Ping Echo Request packets received.

ICMPv6 Echo Reply packets received (icmpv6RxEchoReply) ICMPv6 Ping Echo Reply packets received.

ICMPv6 NA packets transmitted (icmpv6TxNa) ICMPv6 neighbor advertisement packets transmitted. These packets are sent in response to a neighbor solicitation packet, or if the link layer address of this node has changed.

ICMPv6 NS packets transmitted (icmpv6TxNs) ICMPv6 neighbor solicitation packets transmitted. These packets are sent to get the link layer addresses of neighboring nodes or to confirm that they are reachable.

ICMPv6 RA packets transmitted (icmpv6TxRa) ICMPv6 router advertisement packets transmitted. These packets are sent at regular intervals or in response to a router solicitation packet from a neighbor.

ICMPv6 RS packets transmitted (icmpv6TxRs) ICMPv6 router solicitation packets transmitted. These packets are sent to request neighboring routers to generate router advertisements immediately rather than wait for the next defined time.

ICMPv6 Echo Request packets transmitted (icmpv6TxEchoReq) ICMPv6 Ping Echo Request packets transmitted.

ICMPv6 Echo Reply packets transmitted (icmpv6TxEchoReply) ICMP Ping Echo Reply packets transmitted.

ICMPv6 RA error packets (Error in RA packet) ICMPv6 router advertisement error packets received that contain an error in the header, such as an incorrect source IP address, destination IP address, or packet length.

ICMPv6 NA error packets (Error in NA packet) ICMPv6 neighbor advertisement error packets received that contain an error in the header, such as an incorrect source IP address, destination IP address, or packet length.

ICMPv6 NS error packets (Error in NS packet) ICMPv6 neighbor solicitation error packets received that contain an error in the header, such as an incorrect source IP address, destination IP address, or packet length.

ICMPv6 bad checksum (Cksumerr) Packets received with an ICMPv6 checksum error.

unsupported ICMPv6 packets (icmpv6Unspt) ICMPv6 packets received that are not supported by the Citrix ADC.

Rate threshold exceeded packets (icmpv6thsld) Packets dropped because the default threshold of 100 requests per 10 milliseconds has been exceeded. This is a configurable value using the set rateControl command.

Related Commands

- stat protocol http3

protocol-ip

The following operations can be performed on "protocol-ip":

stat protocol ip

Displays statistics of the IP protocol.

Synopsis

stat protocol ip

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

IP packets received (IPPktRx) IP packets received.

IP bytes received (IPbRx) Bytes of IP data received.

IP packets transmitted (IPPktTx) IP packets transmitted.

IP bytes transmitted (IPbTx) Bytes of IP data transmitted.

Megabits received (IPMbRx) Megabits of IP data received.

Megabits transmitted (IPMbTx) Megabits of IP data transmitted.

Total routed IP packets (IPRoutedPkts) Total routed packets.

Total routed IP Mbits (IPRoutedMbits) Total routed Mbits

IP fragments received (IPFragRx) IP fragments received.

Successful reassembly (reasSucc) Fragmented IP packets successfully reassembled on the Citrix ADC.

Reassembly attempted (reasAtmp) IP packets that the Citrix ADC attempts to reassemble. If one of the fragments is missing, the whole packet is dropped.

IP address lookups (IpLkUp) IP address lookups performed by the Citrix ADC. When a packet is received on a non-established session, the Citrix ADC checks if the destination IP address is one of the Citrix ADC owned IP addresses.

IP address lookup failure (IpLkFail) IP address lookups performed by the Citrix ADC that have failed because the destination IP address of the packet does not match any of the Citrix ADC owned IP addresses.

UDP fragments forwarded (udpFgFwd) UDP fragments forwarded to the client or the server.

TCP fragments forwarded (tcpFgFwd) TCP fragments forwarded to the client or the server.

Fragmentation packets created (frgPktCr) Fragmented packets created by the Citrix ADC.

Bad IP checksums (badCksum) Packets received with an IP checksum error.

Unsuccessful reassembly (reasFail) Packets received that could not be reassembled. This can occur when there is a checksum failure, an identification field mismatch, or when one of the fragments is missing.

Reassembled data too big (reasBig) Packets received for which the reassembled data exceeds the Ethernet packet data length of 1500 bytes.

Zero fragment length received (zeroLen) Packets received with a fragment length of 0 bytes.

Duplicate fragments received (dupFrag) Duplicate IP fragments received. This can occur when the acknowledgement was not received within the expected time.

Out of order fragment received (oooFrag) Fragments received that are out of order.

Unknown destination received (UnkDst) Packets received in which the destination IP address was not reachable or not owned by the Citrix ADC.

Bad Transport (badTran) Packets received in which the protocol specified in the IP header is unknown to the Citrix ADC.

VIP down (vipDown) Packets received for which the VIP is down. This can occur when all the services bound to the VIP are down or the VIP is manually disabled.

Fix header failure (hdrFail) Packets received that contain an error in one or more components of the IP header.

TTL expired during transit (ttlExp) Packets for which the time-to-live (TTL) expired during transit. These packets are dropped.

max non-TCP clients (maxClt) Attempts to open a new connection to a service for which the maximum limit has been exceeded. Default value, 0, applies no limit.

Unknown services (UnkSvc) Packets received on a port or service that is not configured.

land-attacks (LndAtk) Land-attack packets received. The source and destination addresses are the same.

Invalid IP header size (errHdrSz) Packets received in which an invalid data length is specified, or the value in the length field and the actual data length do not match. The range for the Ethernet packet data length is 0-1500 bytes.

Invalid IP packet size (errPktLen) Total number of packets received by Citrix ADC with invalid IP packet size.

Truncated IP packet (trIP) Truncated IP packets received. An overflow in the routers along the path can truncate IP packets.

Truncated non-IP packet (trNonIp) Truncated non-IP packets received.

ZERO next hop (zrNxtHop) Packets received that contain a 0 value in the next hop field. These packets are dropped.

Packets with len > 1514 rcvd (BadLenTx) Packets received with a length greater than the normal maximum transmission unit of 1514 bytes.

Packets with bad MAC sent (BadMacTx) IP packets transmitted with a bad MAC address.

Related Commands

- stat protocol http3

protocol-ipv6

The following operations can be performed on "protocol-ipv6":

stat protocol ipv6

Displays statistics of the IPv6 protocol.

Synopsis

stat protocol ipv6

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

IPv6 packets received (ipv6RxPkts) IPv6 packets received.

IPv6 bytes received (ipv6RxBytes) Bytes of IPv6 data received.

IPv6 packets transmitted (ipv6TxPkts) IPv6 packets transmitted

IPv6 bytes transmitted (ipv6TxBytes) Bytes of IPv6 data transmitted.

Total Routed IPv6 packets (ipv6RoutePkts) IPv6 packets routed.

Total Routed IPv6 Mbits (ipv6RouteMbits) IPv6 total Mbits.

IPv6 Fragments received. (ipv6FragRxPkts) IPv6 fragments received.

TCP Fragments reassembled. (ipv6FragTcpReass) TCP fragments processed after reassembly.

UDP Fragments reassembled. (ipv6FragUdpReass) UDP fragments processed after reassembly.

IPv6 Fragments processed without reassembly. (ipv6FragPktsProcessNoReass) IPv6 fragments processed without reassembly.

IPv6 Fragments bridged. (ipv6FragPktsForward) IPv6 fragments forwarded to the client or server without reassembly.

IPv6 error hdr packets (RxErrHdr) Packets received that contain an error in one or more components of the IPv6 header.

IPv6 unsupported next header (Errnxthdr) Packets received that contain an unsupported next header. The supported next headers are TCP, ICMP, UDP, OSPF, and FRAGMENT.

IPv6 Land-attacks (land attack) Land-attack packets received. The source and destination addresses are the same. If not dropped, these packets can lock up the appliance.

Reassembled data too big (AssembledPktTooBig) Packets received for which the reassembled data exceeds the Ethernet packet data length of 1500 bytes.

Zero fragment length received (ZeroLenFramentedPkt) Packets received with a fragment length of 0 bytes.

ICMPv6 NA packets received Number of ICMPv6 NA packets received by Citrix ADC (OBSOLETE).

ICMPv6 NS packets received Number of ICMPv6 NS packets received by Citrix ADC (OBSOLETE).

ICMPv6 NA packets transmitted Number of ICMPv6 NA packets transmitted by Citrix ADC (OBSOLETE).

ICMPv6 NS packets transmitted Number of ICMPv6 NS packets transmitted by Citrix ADC (OBSOLETE).

ICMPv6 RA packets received Number of ICMPv6 RA packets received by Citrix ADC (OBSOLETE).

ICMPv6 RS packets transmitted Number of ICMPv6 RS packets transmitted by Citrix ADC (OBSOLETE).

ICMPv6 packets received Number of ICMPv6 packets received by Citrix ADC (OBSOLETE).

ICMPv6 packets transmitted Number of ICMPv6 packets transmitted by Citrix ADC (OBSOLETE).

IPv6 error hdr packets Number of erroneous header packets received (OBSOLETE).

IPv6 error packets Number of erroneous packets received (OBSOLETE).

IPv6 bad checksum Number of bad checksum packets received (OBSOLETE).

ICMPv6 error packets Number of erroneous ICMPv6 packets received (OBSOLETE).

unsupported ICMPv6 packets Number of ICMPv6 unsupported packets received (OBSOLETE).

Rate threshold exceeded packets Number of ICMPv6 packets dropped for rate threshold exceeded (OBSOLETE).

Related Commands

- stat protocol http3

protocol-mptcp

The following operations can be performed on "protocol-mptcp":

stat protocol mptcp

Displays statistics of the MPTCP protocol.

Synopsis

stat protocol mptcp

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

MPTCP sessions created (TotSess) MPTCP total sessions created

MPTCP V1 sessions created (TotV1Sess) MPTCP total V1 sessions created

Subflow connections created (subCon) MPTCP total Subflow connections created

Current MPTCP sessions The number of current mptcp sessions.

Current V1 MPTCP sessions (CurV1Sess) The number of current V1 mptcp sessions.

Current Subflow connections The number of current mptcp subflow connections.

Pending subflow connections The number of current mptcp subflow connections in pending state.

Sessions without any subflows Current Multipath TCP sessions without any subflows

MP_CAPABLE SYN received (MPSYN) MPTCP total MP_CAPABLE received

MP_CAPABLE V1 SYN received (MPV1SYN) MPTCP total Version1 MP_CAPABLE received

MP_CAPABLE sessions steered (ConSter) Total MP_CAPABLE sessions steered

MP_CAPABLE sessions created (ConReq) Total MP_CAPABLE sessions created.

MP_CAPABLE SYN/ACKs sent (SYNACK) Total number of MP_CAPABLE SYN/ACKs sent.

MP_CAPABLE Final ACKs (FinalACK) Total number of MP_CAPABLE Final ACKs received.

MP_JOIN SYN received (JoinSYN) MPTCP total MP_JOIN syn received

MP_JOIN subflows steered (SFsteer) Total MP_JOIN subflows steered

MP_JOIN SYN/ACKs sent (SFsynack) Total MP_JOIN SYN/ACKs sent.

MP_JOIN Final ACKs (SFFACK) Total number of MP_JOIN Final ACKs

MP_JOIN Final ACK validated (FACKVald) Total number of Subflow final ACK from peer in 3 way handshake validated with 4th ACK.

Established subflows replaced (TotSFRep) MPTCP Total established subflows replaced due to new MP_JOIN.

Pending subflows replaced (PendRep) MPTCP Total pending subflows replaced due to new MP_JOIN.

Fresh ACK on subflow (SFfrhACK) Fresh ACK recieved on a subflow

Fallback to TCP on plain ACK (TotFB) MPTCP Fallback to regular tcp on receiving plain ACK for DSS.

Infinite map set (InfSet) MPTCP Received and set infinite map and fallen back to regular TCP.

Addresses removed with REMOVE_ADDR (REMAddr) Total number of addresses removed from MPTCP connection with REMOVE_ADDR option

DSS(Data Sequence Signal) packets (TotDSS) Total number of Data Sequence Signal packets.

DSS received (DSSrcv) MPTCP Total Data Sequence Signal packets received.

DSS sent (DSSsnd) MMPTCP Total Data Sequence Signal packets sent

DSS with DATA_ACK (DSSA) Total Data Sequence Signal packets during data transfer with DATA_ACK

DSS with 8 octet DATA_ACK (DSSa) Total Data Sequence Signal packets during data transfer with 8 octet DATA_ACK

DSS with Fresh ACK (FreshAck) MPTCP total Data Sequence Signal packets during data transfer with fresh ACK

DSS with Sequence Map (SeqMapM) MPTCP total data Sequence Signal packets with Data Sequence Mapping and checksum

DSS with 8 octet Sequence Map (SeqMapm) MPTCP total data Sequence Signal packets with 8 octet Data Sequence Mapping and checksum

DSS with infinite map flag (InfMapFg) MPTCP received Data Sequence Signal with infinite map flag (Fallback to regular TCP).

Map amount of data not received (LDataLen) MPTCP Map amount of data not yet received.

Subflow used as backup path (PrioBkup) MPTCP Subflow used as backup path.

Clear backup subflow(MP_PRIO) (ClrBkup) Subflow earlier used only as a backup subflow, changes to regular subflow with MP_PRIO option

MP_CAPABLE DATA_FIN sent (TxFin) Total MPTCP connection close requests sent

MP_CAPABLE DATA_FIN received (RxFin) Total MPTCP connection close(DATA_FIN) requests received.

Subflow FIN (SfFin) MPTCP total subflow close requests.

Invalid cookie in MP_CAPABLE ACK (CookieEr) MPTCP invalid cookie received on MP_CAPABLE final ACK.

MP_CAPABLE Extension flag set (ExtnFlEr) Extension flag is set on MP_CAPABLE request.

MP_CAPABLE Reserved flag set (ResFlgEr) MPTCP One or more reserved bits are set on MP_CAPABLE request.

Invalid token in MP_JOIN Request (TokenEr) MPTCP invalid token received on MP_JOIN request.

MP_JOIN on existing address id (AddrIdEr) MPTCP MP_JOIN request on existing address id.

MP_JOIN request with addr id 0 (addridEr) MPTCP MP_JOIN request on address id 0.

MP_JOIN after Maximum subflows (MaxsfEr) MPTCP new MP_JOIN request after maximum configured subflows are established.

MP_JOIN Threshold limit reached (JoinThEr) MPTCP Global pending MP_JOIN threshold limit is reached, new MP_JOIN request will be dropped sending RST

MP_JOIN request after fallback (FBJoinEr) MPTCP New MP_JOIN request received after fallback to regular tcp.

Invalid MAC in MP_JOIN (InMACEr) MPTCP invalid MAC on MP_JOIN final ACK.

Invalid MPTCP option received (OPTEr) MPTCP invalid mptcp option is received and is dropped.

Invalid subtype in option (SubtypEr) Invalid subtype in MPTCP option field and hence discarded.

Option on nonexistent session (OptSesEr) MPTCP options sent on non existing connection/ subflow PCBs.

Invalid remove address ID (REMEr) MPTCP remove address request received on invalid/ unknown address id.

RST on bad options (OptRstEr) MPTCP sent RST on receiving improper option field.

Remove self address (RemSlfEr) MPTCP remove address request for self address.

Add RSS filter failed (RssfEr) Add RSS filter to steer traffic to right node on established MPTCP session failed.

No Payload length (LenEr) MPTCP Payload length not specified in packet.

Unsupported MSS negotiated (MSSErr) MPTCP Unsupported MSS negotiated error.

MPTCP Checksum failure (CksumEr) MPTCP checksum failed. Connection will fallback to regular tcp.

Client crypto algo not supported (CryptoEr) MPTCP client crypto algorithm not supported.

Client version not supported (VerEr) MPTCP MP_CAPABLE request from unsupported mptcp client.

RST subflow on plain ACK (TotPArst) MPTCP Sent RST on receiving plain ACK for DSS.

DATA_FIN on passive subflow (DFpasveEr) MPTCP Data FIN received on passive subflow

Total FAST_CLOSE sent (FCSentEr) MPTCP FAST CLOSE sent.

FAST_CLOSE on passive subflow (FCpasvEr) MPTCP Fast close received on passive subflow.

FAST_CLOSE received (FCRcvEr) MPTCP FAST_CLOSE received on a subflow.

FAST_CLOSE with invalid key (FCkeyEr) MPTCP FAST_CLOSE received with invalid key and the packet is dropped.

MP_FAIL sent (MPFAILst) MPTCP Total MP_FAIL sent due to checksum failure.

MP_FAIL received (MPFAILrv) MPTCP Total MP_FAIL received and fallback to regular TCP.

Packet without Sequence mapping (NomapEr) MPTCP Packet received with no Data Sequence Mapping.

More data than Sequence mapping (MrDataEr) MPTCP More data received than the available Data Sequence Mapping.

Invalid Sequence Map (InMapEr) MPTCP Drop the session incase of invalid Data Sequence map.

Duplicate Sequence Map (DupmapEr) MPTCP Duplicate maps in Data Sequence map table.

Invalid subflow sequence (SfnEr) MPTCP subflow map doesn't exactly match MPTCP session mapping.

Received bad sequence map (BadMapEr) MPTCP sequence map already exists.

Retransmitted Data Recevied (RetxEr) Retransmitted Data Recevied on MPTCP session.

Subflow MEM ALLOC Fail (SfMemEr) Attaching the subflow to MPTCP session failed due to failure in allocating memory to subflow map table.

Session MEM ALLOC Fail (SesMemEr) Creating a MPTCP connection failed due to failure in allocating memory to MPTCP connection management structure.

Subflow connection ALLOC Fail (SfPcbEr) Allocating memory to TCP protocol control block(PCB) for subflow failed.

Session connection ALLOC Fail (MpcbEr) Allocating memory to MPTCP protocol control block failed.

Output packet MEM ALLOC Fail (PktMemEr) Failed to allocate memory to output MPTCP packet.

Output packet without subflow (PktSfEr) MPTCP output a packet without any subflow PCB.

MPTCP V1 Invalid Data_Key Seq (V1DataPriorToKey) MPTCP V1 data received prior to key

Related Commands

- stat protocol http3

protocol-quic

The following operations can be performed on "protocol-quic":

stat protocol quic

Displays statistics of the QUIC protocol.

Synopsis

stat protocol quic

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Client UDP Datagrams rcvd (QuicClntDgrmRcvd) Total QUIC client UDP datagrams received

Server UDP Datagrams rcvd (QuicSvrDgrmRcvd) Total QUIC server UDP datagrams received

Client UDP Datagrams sent (QuicClntDgrmSent) Total QUIC client UDP datagrams sent

Server UDP Datagrams sent (QuicSvrDgrmSent) Total QUIC server UDP datagrams sent

Client connections (QuicCurClntConn) Current QUIC client connections

Server connections (QuicCurSvrConn) Current QUIC server connections

Local Conn IDs allocated (QuicLclConnID) Current QUIC local connection IDs allocated

Async Crypto contexts allocated (QuicCurSavedCryptoCtx) Current QUIC crypto contexts allocated

Client connections (QuicTotClntConn) Total QUIC client connections

Server connections (QuicTotSvrConn) Total QUIC server connections

Migrated QUIC connections (QuicMigConn) Total number of migrated QUIC connections

Jumbo frames rcvd (QuicJMBFrRcvd) Total number of QUIC jumbo frames received

Retry pkts sent (QuicRetPktSent) Number of QUIC Retry packets sent

Handshake messages completed (QuicHndShkCmpltd) Number of QUIC handshake messages completed

Trans Conn Close pkts sent (QuicTrnsptConnClPktSent) Number of QUIC transport no-error Connection Close packets sent

App Conn Close pkts sent (QuicAppConnClPktSent) Number of QUIC application no-error Connection Close packets sent

Async Datagrams Sent (QuicAsyncDatagramsSent) Number of QUIC datagrams sent using async mode

Session allocations failed (QuicConninfAlcFail) Quic session allocations failed

NSB allocations failed (QuicNSBAlcFail) Quic NSB allocations failed

TLS transport errors sent (QuicTLSAlrtSent) Total QUIC TLS 1.3 transport errors sent

Stateless Conn Close pkts sent (QuicStlessConnClPktSent) Number of QUIC stateless Connection Close packets sent

Version Negotiation pkts sent (QuicVerNegPktSent) Number of QUIC Version Negotiation packets sent

Trans Conn Close pkts failed (QuicTrnsptConnClPktFail) Number of QUIC transport error Connection Close packets sent

App Conn Close pkts failed (QuicAppConnClPktFail) Number of QUIC application error Connection Close packets sent

Retry token verification failed (QuicRetTknVerFail) Number of times QUIC Retry token verification failed

NEW_TOKEN verification failed (QuicNewTknVerFail) Number of times QUIC NEW_TOKEN token verification failed

Related Commands

- stat protocol http3

protocol-quicbridge

The following operations can be performed on "protocol-quicbridge":

stat protocol quicbridge

Displays statistics of the QUIC BRIDGE protocol.

Synopsis

stat protocol quicbridge

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Connections (QuicBConn) Total number of QUIC Bridge connections

Migrated Connections (QuicBMigConn) Total number of migrated QUIC Bridge connections

Connection infos (QuicBqci) Current number of QUIC Bridge connection infos

Peer infos (QuicBqpi) Current number of QUIC Bridge peer infos

Peer info alloc fails (QuicBqpiAlcFail) Number of QUIC Bridge peer info allocation failures

Conn info alloc fails (QuicBqciAlcFail) Number of QUIC Bridge connection info allocation failures

Related Commands

- stat protocol http3

protocol-tcp

The following operations can be performed on "protocol-tcp":

stat protocol tcp

Displays statistics of the TCP protocol.

Synopsis

stat protocol tcp

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Server active connections (ActSvrCo) Connections to a server currently responding to requests.

Opening server connections (SvrCxO) Server connections in the Opening state, which indicates that the handshakes are not yet complete.

Opening client connections (CltCxO) Client connections in the Opening state, which indicates that the handshakes are not yet complete.

Established client connections (CltCxE) Current client connections in the Established state, which indicates that data transfer can occur between the Citrix ADC and the client.

Established server connections (SvrCxE) Current server connections in the Established state, which indicates that data transfer can occur between the Citrix ADC and the server.

TCP packets received (TCPPktRx) TCP packets received.

TCP bytes received (TCPbRx) Bytes of TCP data received.

TCP packets transmitted (TCPPktTx) TCP packets transmitted.

TCP bytes transmitted (TCPbTx) Bytes of TCP data transmitted.

All client connections (CltCx) Client connections, including connections in the Opening, Established, and Closing state.

Closing client connections (CltCxCl) Client connections in the Closing state, which indicates that the connection termination process has initiated but is not complete.

Opened client connections (TotCltO) Client connections opened by the Citrix ADC since startup (after three-way handshake). This counter is reset when the Citrix ADC is restarted.

All server connections (SvrCx) Server connections, including connections in the Opening, Established, and Closing state.

Closing server connections (SvrCxCl) Server connections in the Closing state, which indicates that the connection termination process has initiated but is not complete.

Opened server connections (TotSvrO) Server connections initiated by the Citrix ADC since startup. This counter is reset when the Citrix ADC is restarted.

Surge queue (SQlen) Connections in the surge queue. When the Citrix ADC cannot open a connection to the server, for example when maximum connections have been reached, the Citrix ADC queues these requests.

Spare connections (SpConn) Spare connections available. To save time and resources in establishing another connection for a new client, the connection on the server is not closed after completing the request from the first client and is available for serving future requests.

Client idle flushed (ZomCltF) Client connections that are flushed because the client has been idle for some time.

Client half opened flushed (ZCltFHo) Half-opened client connections that are flushed because the three-way handshakes are not complete.

Client active half closed flushed (ZCltFAhc) Active half-closed client connections that are flushed because the client has closed the connection and there has been no activity on the connection.

Client passive half closed flushed (ZCltFPhc) Passive half-closed client connections that are flushed because the Citrix ADC has closed the connection and there has been no activity on the connection.

Server idle connections flushed (ZSvrF) Server connections that are flushed because there have been no client requests in the queue for some time.

Server half opened flushed (ZSvrFHo) Half-opened server connections that are flushed because the three-way handshakes are not complete.

Server active half closed flushed (ZSvrFAhc) Active half-closed server connections that are flushed because the server has closed the connection and there has been no activity on the connection.

Server passive half closed flushed (ZSrvFPhc) Passive half-closed server connections that are flushed because the Citrix ADC has closed the connection and there has been no activity on the connection.

Zombie cleanup calls (ZmbCall) Times the Zombie cleanup function is called. Every time a connection is flushed, it is marked for cleanup. The Zombie cleanup function clears all these connections at predefined intervals.

SYN packets received (TCPSYN) SYN packets received

Server probes (SYNProbe) Probes from the Citrix ADC to a server. The Citrix ADC sends a SYN packet to the server to check its availability and expects a SYN_ACK packet from the server before a specified response timeout.

FIN packets from server (SvrFin) FIN packets received from the server.

FIN packets from client (CltFin) FIN packets received from the clients.

Time wait to SYN (WaToSyn) SYN packets (packets used to initiate a TCP connection) received on connections that are in the TIME_WAIT state. Packets cannot be transferred on a connection in this state.

Data in TIME_WAIT (WaDat) Bytes of data received on connections that are in the TIME_WAIT state. Data cannot be transferred on a connection that is in this state.

SYN packets held (SYNHeld) SYN packets held on the Citrix ADC that are waiting for a server connection.

SYN packets flushed (SYNFlush) SYN packets flushed on the Citrix ADC because of no response from the server for three or more seconds.

TIME_WAIT connections closed (FinWaitC) Connections closed on the Citrix ADC because the number of connections in the TIME_WAIT state has exceeded the default value of 7000.

Bad TCP checksum (TCPBadCk) Packets received with a TCP checksum error.

Data after FIN (TCPDtFin) Packets received following a connection termination request. This error is usually caused by a reordering of packets during transmission.

SYN in SYN_RCVD state (TCPSYNRv) SYN packets received on a connection that is in the SYN_RCVD state. A connection goes into the SYN_RCVD state after receiving a SYN packet.

SYN in ESTABLISHED state (TCPSYNEs) SYN packets received on a connection that is in the ESTABLISHED state. A SYN packet is not expected on an ESTABLISHED connection.

SYN_SENT incorrect ACK packet (TCPBadAk) Incorrect ACK packets received on a connection that is in the SYN_SENT state. An incorrect ACK packet is the third packet in the three-way handshake that has an incorrect sequence number.

RST packets received (TCPRST) Reset packets received from a client or a server.

RST on not ESTABLISHED (TCPRSTNE) Reset packets received on a connection that is not in the ESTABLISHED state.

RST out of window (TCPRSTOW) Reset packets received on a connection that is out of the current TCP window.

RST in TIME_WAIT (TCPRSTTi) Reset packets received on a connection that is in the TIME_WAIT state. Packets cannot be transferred on a connection in the TIME_WAIT state.

Server out of order packets (SvrOOO) Out of order TCP packets received from a server.

Client out of order packets (CltOOO) Out of order TCP packets received from a client.

TCP hole on client connection (CltHole) TCP holes created on a client connection. When out of order packets are received from a client, a hole is created on the Citrix ADC for each group of missing packets.

TCP hole on server connection (SvrHole) TCP holes created on a server connection. When out of order packets are received from a server, a hole is created on the Citrix ADC for each group of missing packets.

Seq number SYN cookie reject (CSeqRej) SYN cookie packets rejected because they contain an incorrect sequence number.

Signature SYN cookie reject (CSigRej) SYN cookie packets rejected because they contain an incorrect signature.

Seq number SYN cookie drop (CSigDrp) SYN cookie packets dropped because the sequence number specified in the packets is outside the current window.

MSS SYN cookie reject (CMssRej) SYN cookie packets rejected because the maximum segment size (MSS) specified in the packets is incorrect.

Any IP port allocation failure (PortFal) Port allocations that have failed on a mapped IP address because the maximum limit of 65536 has been exceeded.

IP port allocation failure (PortFalI) Port allocations that have failed on a subnet IP address or vserver IP address because the maximum limit of 65536 has been exceeded.

Stray packets (StrayPkt) Number of stray or misrouted packets.

RST packets sent (SentRst) Reset packets sent to a client or a server.

Bad state connections (BadConn) Connections that are not in a valid TCP state.

RST threshold dropped (RstThre) Reset packets dropped because the default threshold of 100 resets per 10 milliseconds has been exceeded. This is a configurable value using the set rateControl command.

Packets out of window (OOWPkt) Packets received that are out of the current advertised window.

SYNs dropped (Congestion) (SynCng) SYN packets dropped because of network congestion.

Client retransmissions (TCPCltRe) Packets retransmitted by a client. This usually occurs because the acknowledgement from the Citrix ADC has not reached the client.

Full packet retransmissions (TCPFulRe) Full packets retransmitted by the client or the server.

SYN packet retries (TCPSYNRe) SYN packets resent to a server.

SYN packets timeout (TCPSYNG) Attempts to establish a connection on the Citrix ADC that timed out.

TCP retransmission (Retr) TCP packets retransmitted. The Citrix ADC attempts to retransmit the packet up to seven times, after which it resets the other half of the TCP connection.

1st retransmission (1stRetr) Packets retransmitted once by the Citrix ADC.

3rd retransmission (3rdRetr) Packets retransmitted three times by the Citrix ADC.

5th retransmission (5thRetr) Packets retransmitted five times by the Citrix ADC.

7th retransmission (7thRetr) Packets retransmitted seven times by the Citrix ADC. If this fails, the Citrix ADC terminates the connection.

Fast retransmits (FastRetr) TCP packets on which the Citrix ADC performs a fast retransmission in response to three duplicate acknowledgements or a partial acknowledgement. The Citrix ADC assumes that the packet is lost and retransmits the packet before its time-out.

Server retransmissions (TCPSvrRe) Packets retransmitted by a server. This usually occurs because the acknowledgement from the Citrix ADC has not reached the server.

Partial packet retransmissions (TCPParRe) Partial packet retransmits by a client or server due to congestion on the connection. This usually occurs because the window advertised by the Citrix ADC is not big enough to hold the full packet.

FIN packet retries (TCPFINRe) FIN packets resent to a server or a client.

FIN packets timeout (TCPFING) Connections that were timed out by the Citrix ADC because of not receiving the ACK packet after retransmitting the FIN packet four times.

2nd retransmission (2ndRetr) Packets retransmitted twice by the Citrix ADC.

4th retransmission (4thRetr) Packets retransmitted four times by the Citrix ADC.

6th retransmission (6thRetr) Packets retransmitted six times by the Citrix ADC.

TCP retransmission giveup (RetrG) Number of times Citrix ADC terminates a connection after retransmitting the packet seven times on that connection.Retrasnmission happens when recieving end doesn't acknowledges the packet.

TCP level cip failure (CltHdrEr) Number of times TCP level client header insertion failure

Related Commands

- stat protocol http3

protocol-udp

The following operations can be performed on "protocol-udp":

stat protocol udp

Displays statistics of the UDP protocol.

Synopsis

stat protocol udp

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Packets received (UDPPktRx) Total number of UDP packets received.

Bytes received (UDPbRx) Total number of UDP data received in bytes.

Packets transmitted (UDPPktTx) Total number of UDP packets transmitted.

Bytes transmitted (UDPbTx) Total number of UDP data transmitted in bytes.

Current rate threshold (UDPThs) Limit for UDP packets handled every 10 milliseconds. Default value, 0, applies no limit. This is a configurable value using the set rateControl command.

Unknown service (UDPUnSvc) Stray UDP packets dropped due to no configured listening service.

Bad UDP checksum (UDPBadCkSum) Packets received with a UDP checksum error.

Rate threshold exceeded (UDPRtEx) Number of times the UDP rate threshold is exceeded. If this counter continuously increases, first make sure the UDP packets received are genuine. If they are, increase the current rate threshold. This is a configurable value using the set rateControl command.

Related Commands

- stat protocol http3

qos

Qos

The entities on which you can perform NetScaler CLI operations:

- qos
- qos-stats

qos-stats

The following operations can be performed on "qos-stats":

show qos stats

show qos stats is an alias for stat qos

Synopsis

show qos stats - alias for 'stat qos'

qos

The following operations can be performed on "qos":

stat qos

Display QoS statistics.

Synopsis

stat qos

Arguments

name detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Receive direction packets processed by QoS (qos_packets_received) Receive direction packets processed by QoS

Send direction packets processed by QoS (qos_packets_sent) Send direction packets processed by QoS

Packets bypassing QoS (qos_packets_bypassed) Packets bypassing QoS

Total packets dropped (qos_packets_dropped) Total packets dropped

Received bytes processed by QoS (qos_bytes_rx) Received bytes processed by QoS

Sent bytes processed by QoS (qos_bytes_tx) Sent bytes processed by QoS

QoS lazy byte optimization rate (qos_lazy_bytes) QoS lazy byte optimization rate

QoS actual bytes scheduled (qos_real_bytes) QoS actual bytes scheduled

Total packets filtered by QoS (qos_packets_filtered) Total packets filtered by QoS

Total packets classified by QoS (qos_packets_classified) Total packets classified by QoS

New QoS flows (qos_flows) New QoS flows

Recycled QoS flows (qos_flow_recycles) Recycled QoS flows

QoS Flow Recycle failures (qos_session_recycle_failure) QoS Flow Recycle failures

Sessions manually ignored (qos_sessions_ignored) Sessions manually ignored

sessions manually consumed (qos_sessions_consumed) sessions manually consumed

Uneque qos action objects created (qos_actions_created) Uneque qos action objects created

Policies re-evaluated due to cli change (qos_policy_reeval) Policies re-evaluated due to cli change

Connections unable to be classified beyond TCP (qos_cfy_tcp_unknown) Connections unable to be classified beyond TCP

Connections unable to be classified beyond UDP (qos_cfy_udp_unknown) Connections unable to be classified beyond UDP

Scheduler leaf nodes constructed (qos_sch_leafs) Scheduler leaf nodes constructed

Session memory allocated (qos_session_mem) Session memory allocated

Scheduler virtual packets constructed (qos_sch_virtual_packets) Scheduler virtual packets constructed

Scheduler bytes accepted (qos_sch_virtual_bytes_accepted) Scheduler bytes accepted

Scheduler Failures to recycle QoS flows (qos_sch_leaf_recycle_failures) Scheduler Failures to recycle QoS flows

Scheduler Regulated node count (qos_sch_node_regulated_count) Scheduler Regulated node count

Scheduler session classes constructed (qos_sch_sessions_created) Scheduler session classes constructed

Scheduler session classes constructed (qos_sch_sessions_deleted) Scheduler session classes constructed

Scheduler sdrr nodes constructed (qos_sch_sdrr_nodes) Scheduler sdrr nodes constructed

Scheduler session connections created (qos_sch_session_conns) Scheduler session connections created

Scheduler session connections removed (qos_sch_session_conns_removed) Scheduler session connections removed

Scheduler regulated sessions count (qos_sch_sessions_regulated_count) Scheduler regulated sessions count

Scheduler session bytes total (qos_sch_sessions_byte_count) Scheduler session bytes total

Scheduler regulated node count (qos_sch_regulated_count) Scheduler regulated node count

Scheduler links created (qos_sch_links_created) Scheduler links created

Scheduler links deleted (qos_sch_links_deleted) Scheduler links deleted

Scheduler links updated (qos_sch_links_updated) Scheduler links updated

Scheduler calls to poll_libqos (qos_sch_poll_count) Scheduler calls to poll_libqos

Scheduler peer messages received (qos_sch_peer_msgs) Scheduler peer messages received

IPC failed for QoS messages. (qos_error_ipc) IPC failed for QoS messages.

Flow memory allocated (qos_flow_mem) Flow memory allocated

Flows free list size (qos_flows_available) Flows free list size

Recycle failed due to backlog (qos_recycle_failed_backlog) Recycle failed due to backlog

Recycle failed due to session attachment (qos_recycle_failed_session) Recycle failed due to session attachment

Failed attempts to create actions (qos_error_create_action_failed) Failed attempts to create actions

Failed attempts to modify actions (qos_error_modify_action_failed) Failed attempts to modify actions

Failed attempts to remove actions (qos_error_remove_action_failed) Failed attempts to remove actions

Internal CLI error (qos_error_cli_unknown) Internal CLI error

qos action rename not yet implemented (qos_error_rename_not_implemented) qos action rename not yet implemented

Failed attempts to remove qos policy (qos_error_remove_policy_failed) Failed attempts to remove qos policy

Failed attempts to create qos policy (qos_error_create_policy_failed) Failed attempts to create qos policy

Libqos api failures (qos_error_libqos_api_failures) Libqos api failures

Libqos api qos_session_add_pcb/natpcb() failed for reason QS_EINVALIDPCB (qos_error_api_ses_invalidpcb) Libqos api qos_session_add_pcb/natpcb() failed for reason QS_EINVALIDPCB

Libqos api qos_session_add_pcb/natpcb() failed for reason QS_ENOTREADY (qos_error_api_ses_notready) Libqos api qos_session_add_pcb/natpcb() failed for reason QS_ENOTREADY

Libqos api qos_session_add_pcb/natpcb() failed for reason QS_EINSESSION (qos_error_api_ses_add_insession) Libqos api qos_session_add_pcb/natpcb() failed for reason QS_EINSESSION

Libqos api qos_session_add_pcb/natpcb() failed (qos_error_api_ses_add_other) Libqos api qos_session_add_pcb/natpcb() failed

Libqos api qos_session_rem_pcb/natpcb() failed for reason QS_ENOTINSESSION (qos_error_api_ses_rem_notinsession) Libqos api qos_session_rem_pcb/natpcb() failed for reason QS_ENOTINSESSION

Libqos api qos_session_rem_pcb/natpcb() failed (qos_error_api_ses_rem_other) Libqos api qos_session_rem_pcb/natpcb() failed

Libqos api qos_session_delete faled (qos_error_api_ses_del) Libqos api qos_session_delete faled

Libqos out of flow memory (qos_error_no_flows) Libqos out of flow memory

Libqos out of session memory (qos_error_no_sessions) Libqos out of session memory

quic

Quic

The entities on which you can perform NetScaler CLI operations:

- quic-param
- quic-profile

quic-param

The following operations can be performed on "quic-param":

unset| set| show|

unset quic param

Use this command to remove quic param settings.Refer to the set quic param command for meanings of the arguments.

Synopsis

unset quic param -quicSecretTimeout

set quic param

Sets the QUIC parameters for the Citrix ADC.

Synopsis

set quic param -quicSecretTimeout <secs>

Arguments

quicSecretTimeout Rotation frequency, in seconds, for the secret used to generate address validation tokens that will be issued in QUIC Retry packets and QUIC NEW_TOKEN frames sent by the Citrix ADC. A value of 0 can be configured if secret rotation is not desired. Default value: 3600 Minimum value: 0 Maximum value: 31536000

show quic param

Displays the QUIC parameters configured on the Citrix ADC.

Synopsis

show quic param

Arguments

Output

quicSecretTimeout Rotation frequency, in seconds, for the secret used to generate address validation tokens that will be issued in QUIC Retry packets and QUIC NEW_TOKEN frames sent by the Citrix ADC. A value of 0 can be configured if secret rotation is not desired.

quic-profile

The following operations can be performed on "quic-profile":

set| show| unset| rm| add|

set quic profile

Modify QUIC profile parameter values of the specified QUIC profile.

Synopsis

set quic profile <name>

Arguments

name Name for the QUIC profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),equals sign (=), and hyphen (-) characters. Cannot be changed after the profile is created.

ackDelayExponent An integer value advertised by the Citrix ADC to the remote QUIC endpoint, indicating an exponent that the remote QUIC endpoint should use, to decode the ACK Delay field in QUIC ACK frames sent by the Citrix ADC. Default value: 3 Minimum value: 0 Maximum value: 20

activeConnectionIDlimit An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the maximum number of QUIC connection IDs from the remote QUIC

endpoint, that the Citrix ADC is willing to store. Default value: 3 Minimum value: 2 Maximum value: 8

activeConnectionMigration Specify whether the Citrix ADC should allow the remote QUIC endpoint to perform active QUIC connection migration.

Possible values: ENABLED, DISABLED Default value: ENABLED

congestionCtrlAlgorithm Specify the congestion control algorithm to be used for QUIC connections. The default congestion control algorithm is CUBIC.

Possible values: Default, NewReno, CUBIC, BBR Default value: Default

initialMaxData An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial value, in bytes, for the maximum amount of data that can be sent on a QUIC connection. Default value: 1048576 Minimum value: 8192 Maximum value: 67108864

initialMaxStreamDataBidiLocal An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial flow control limit, in bytes, for bidirectional QUIC streams initiated by the Citrix ADC. Default value: 262144 Minimum value: 8192 Maximum value: 8388608

initialMaxStreamDataBidiRemote An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial flow control limit, in bytes, for bidirectional QUIC streams initiated by the remote QUIC endpoint. Default value: 262144 Minimum value: 8192 Maximum value: 8388608

initialMaxStreamDataUni An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial flow control limit, in bytes, for unidirectional streams initiated by the remote QUIC endpoint. Default value: 262144 Minimum value: 8192 Maximum value: 8388608

initialMaxStreamsBidi An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial maximum number of bidirectional streams the remote QUIC endpoint may initiate. Default value: 100 Minimum value: 1 Maximum value: 500

initialMaxStreamsUni An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial maximum number of unidirectional streams the remote QUIC endpoint may initiate. Default value: 10 Minimum value: 1 Maximum value: 500

maxAckDelay An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the maximum amount of time, in milliseconds, by which the Citrix ADC will delay sending acknowledgments. Default value: 20 Minimum value: 10 Maximum value: 2000

maxIdleTimeout An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the maximum idle timeout, in seconds, for a QUIC connection. A QUIC connection will be silently discarded by the Citrix ADC if it remains idle for longer than the minimum of the idle timeout values advertised by the Citrix ADC and the remote QUIC endpoint, and three times the current Probe Timeout (PTO). Default value: 180 Minimum value: 1 Maximum value: 3600

maxUDPDatagramsPerBurst An integer value, specifying the maximum number of UDP datagrams that can be transmitted by the Citrix ADC in a single transmission burst on a QUIC connection. Default value: 8 Minimum value: 1 Maximum value: 256

maxUDPPayloadSize An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the size of the largest UDP datagram payload, in bytes, that the Citrix ADC is willing to receive on a QUIC connection. Default value: 1472 Minimum value: 1252 Maximum value: 9188

newTokenValidityPeriod An integer value, specifying the validity period, in seconds, of address validation tokens issued through QUIC NEW_TOKEN frames sent by the Citrix ADC. Default value: 300 Minimum value: 1 Maximum value: 3600

retryTokenValidityPeriod An integer value, specifying the validity period, in seconds, of address validation tokens issued through QUIC Retry packets sent by the Citrix ADC. Default value: 10 Minimum value: 1 Maximum value: 120

statelessAddressValidation Specify whether the Citrix ADC should perform stateless address validation for QUIC clients, by sending tokens in QUIC Retry packets during QUIC connection establishment, and by sending tokens in QUIC NEW_TOKEN frames after QUIC connection establishment.

Possible values: ENABLED, DISABLED Default value: ENABLED

Example

set quic profile <profile name> -statelessAddressValidation DISABLED -maxIdleTimeout 120

show quic profile

Display the parameter values of all the configured QUIC profiles in the system. To display the parameter values of a particular QUIC profile, specify its name.

Synopsis

show quic profile

Arguments

name Name for the QUIC profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),equals sign (=), and hyphen (-) characters. Cannot be changed after the profile is created.

Output

ackDelayExponent An integer value advertised by the Citrix ADC to the remote QUIC endpoint, indicating an exponent that the remote QUIC endpoint should use, to decode the ACK Delay field in QUIC ACK frames sent by the Citrix ADC.

activeConnectionIDlimit An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the maximum number of QUIC connection IDs from the remote QUIC endpoint, that the Citrix ADC is willing to store.

activeConnectionMigration Specify whether the Citrix ADC should allow the remote QUIC endpoint to perform active QUIC connection migration.

congestionCtrlAlgorithm Specify the congestion control algorithm to be used for QUIC connections. The default congestion control algorithm is CUBIC.

initialMaxData An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial value, in bytes, for the maximum amount of data that can be sent on a QUIC connection.

initialMaxStreamDataBidiLocal An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial flow control limit, in bytes, for bidirectional QUIC streams initiated by the Citrix ADC.

initialMaxStreamDataBidiRemote An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial flow control limit, in bytes, for bidirectional QUIC streams initiated by the remote QUIC endpoint.

initialMaxStreamDataUni An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial flow control limit, in bytes, for unidirectional streams initiated by the remote QUIC endpoint.

initialMaxStreamsBidi An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial maximum number of bidirectional streams the remote QUIC endpoint may initiate.

initialMaxStreamsUni An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial maximum number of unidirectional streams the remote QUIC endpoint may initiate.

maxAckDelay An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the maximum amount of time, in milliseconds, by which the Citrix ADC will delay sending acknowledgments.

maxIdleTimeout An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the maximum idle timeout, in seconds, for a QUIC connection. A QUIC connection will be silently discarded by the Citrix ADC if it remains idle for longer than the minimum of the idle timeout values advertised by the Citrix ADC and the remote QUIC endpoint, and three times the current Probe Timeout (PTO).

maxUDPDatagramsPerBurst An integer value, specifying the maximum number of UDP datagrams that can be transmitted by the Citrix ADC in a single transmission burst on a QUIC connection.

maxUDPPayloadSize An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the size of the largest UDP datagram payload, in bytes, that the Citrix ADC is willing to receive on a QUIC connection.

newTokenValidityPeriod An integer value, specifying the validity period, in seconds, of address validation tokens issued through QUIC NEW_TOKEN frames sent by the Citrix ADC.

retryTokenValidityPeriod An integer value, specifying the validity period, in seconds, of address validation tokens issued through QUIC Retry packets sent by the Citrix ADC.

statelessAddressValidation Specify whether the Citrix ADC should perform stateless address validation for QUIC clients, by sending tokens in QUIC Retry packets during QUIC connection establishment, and by sending tokens in QUIC NEW_TOKEN frames after QUIC connection establishment.

refCnt Number of entities using this profile

builtin Flag to determine if the QUIC profile is built-in or not

feature The feature to be checked while applying this config

stateflag State flag

devno count

Example

show quic profile

unset quic profile

Use this command to remove quic profile settings.Refer to the set quic profile command for meanings of the arguments.

Synopsis

unset quic profile <name>

rm quic profile

Remove a QUIC profile on the Citrix ADC

Synopsis

rm quic profile <name>

Arguments

name Name for the QUIC profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),equals sign (=), and hyphen (-) characters. Cannot be changed after the profile is created.

Example

rm quic profile <profile name>

add quic profile

Create a new QUIC profile on the Citrix ADC.

Synopsis

add quic profile <name>

Arguments

name Name for the QUIC profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),equals sign (=), and hyphen (-) characters. Cannot be changed after the profile is created.

ackDelayExponent An integer value advertised by the Citrix ADC to the remote QUIC endpoint, indicating an exponent that the remote QUIC endpoint should use, to decode the ACK Delay field in QUIC ACK frames sent by the Citrix ADC. Default value: 3 Minimum value: 0 Maximum value: 20

activeConnectionIDlimit An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the maximum number of QUIC connection IDs from the remote QUIC endpoint, that the Citrix ADC is willing to store. Default value: 3 Minimum value: 2 Maximum value: 8

activeConnectionMigration Specify whether the Citrix ADC should allow the remote QUIC endpoint to perform active QUIC connection migration.

Possible values: ENABLED, DISABLED Default value: ENABLED

congestionCtrlAlgorithm Specify the congestion control algorithm to be used for QUIC connections. The default congestion control algorithm is CUBIC.

Possible values: Default, NewReno, CUBIC, BBR Default value: Default

initialMaxData An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial value, in bytes, for the maximum amount of data that can be sent on a QUIC connection. Default value: 1048576 Minimum value: 8192 Maximum value: 67108864

initialMaxStreamDataBidiLocal An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial flow control limit, in bytes, for bidirectional QUIC streams initiated by the Citrix ADC. Default value: 262144 Minimum value: 8192 Maximum value: 8388608

initialMaxStreamDataBidiRemote An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial flow control limit, in bytes, for bidirectional QUIC streams initiated by the remote QUIC endpoint. Default value: 262144 Minimum value: 8192 Maximum value: 8388608

initialMaxStreamDataUni An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial flow control limit, in bytes, for unidirectional streams initiated by the remote QUIC endpoint. Default value: 262144 Minimum value: 8192 Maximum value: 8388608

initialMaxStreamsBidi An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial maximum number of bidirectional streams the remote QUIC endpoint may initiate. Default value: 100 Minimum value: 1 Maximum value: 500

initialMaxStreamsUni An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial maximum number of unidirectional streams the remote QUIC endpoint may initiate. Default value: 10 Minimum value: 1 Maximum value: 500

maxAckDelay An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the maximum amount of time, in milliseconds, by which the Citrix ADC will delay sending acknowledgments. Default value: 20 Minimum value: 10 Maximum value: 2000

maxIdleTimeout An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the maximum idle timeout, in seconds, for a QUIC connection. A QUIC connection will be silently discarded by the Citrix ADC if it remains idle for longer than the minimum of the idle timeout values advertised by the Citrix ADC and the remote QUIC endpoint, and three times the current Probe Timeout (PTO). Default value: 180 Minimum value: 1 Maximum value: 3600

maxUDPDatagramsPerBurst An integer value, specifying the maximum number of UDP datagrams that can be transmitted by the Citrix ADC in a single transmission burst on a QUIC connection. Default value: 8 Minimum value: 1 Maximum value: 256

maxUDPPayloadSize An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the size of the largest UDP datagram payload, in bytes, that the Citrix ADC is willing to receive on a QUIC connection. Default value: 1472 Minimum value: 1252 Maximum value: 9188

newTokenValidityPeriod An integer value, specifying the validity period, in seconds, of address validation tokens issued through QUIC NEW_TOKEN frames sent by the Citrix ADC. Default value: 300 Minimum value: 1 Maximum value: 3600

retryTokenValidityPeriod An integer value, specifying the validity period, in seconds, of address validation tokens issued through QUIC Retry packets sent by the Citrix ADC. Default value: 10 Minimum value: 1 Maximum value: 120

statelessAddressValidation Specify whether the Citrix ADC should perform stateless address validation for QUIC clients, by sending tokens in QUIC Retry packets during QUIC connection establishment, and by sending tokens in QUIC NEW_TOKEN frames after QUIC connection establishment.

Possible values: ENABLED, DISABLED Default value: ENABLED

Example

add quic profile <profile name>

quicBridge-profile

The following operations can be performed on "quicBridge-profile":

set| rm| add| unset| show|

set quicBridge profile

Set/modify QUICBRIDGE profile values

Synopsis

set quicBridge profile <name>

Arguments

name Name for the QUIC profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),equals sign (=), and hyphen (-) characters. Cannot be changed after the profile is created.

routingAlgorithm Routing algorithm to generate routable connection IDs.

Possible values: PLAINTEXT Default value: PLAINTEXT

ServerIdlength Length of serverid to encode/decode server information Default value: 4 Minimum value: 2 Maximum value: 38

Example

set quicBridgeprofile <profile name> -quicBridgeRoutingAlgorithm PLAINTEXT -quicBridgeServerIdlength 4

rm quicBridge profile

Remove a QUICBRIDGE profile on the Citrix ADC

Synopsis

rm quicBridge profile <name>

Arguments

name Name for the QUIC profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space,

colon (:), at (@),equals sign (=), and hyphen (-) characters. Cannot be changed after the profile is created.

Example

rm quicBridgeprofile <profile name>

add quicBridge profile

Create a new QUICBRIDGE profile on the Citrix ADC.

Synopsis

add quicBridge profile <name>

Arguments

name Name for the QUIC profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),equals sign (=), and hyphen (-) characters. Cannot be changed after the profile is created.

routingAlgorithm Routing algorithm to generate routable connection IDs.

Possible values: PLAINTEXT Default value: PLAINTEXT

ServerIdlength Length of serverid to encode/decode server information Default value: 4 Minimum value: 2 Maximum value: 38

Example

add quicBridgeProfile quic_prof_1 -quicBridgeRoutingAlgorithm PLAINTEXT -quicBridgeServerIdlength 4

unset quicBridge profile

Removes the attributes of the QUIC Bridge profile. Attributes for which a default value is available revert to their default values. Refer to the 'set ns quicBridge Profile' command for a description of the parameters..Refer to the set quicBridge profile command for meanings of the arguments.

Synopsis

unset quicBridge profile <name>

show quicBridge profile

Display all the configured QUICBRDIGE profiles in the system. If a name is specified, then only that profile is shown.

Synopsis

show quicBridge profile

Arguments

name Name for the QUIC profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),equals sign (=), and hyphen (-) characters. Cannot be changed after the profile is created.

Output

routingAlgorithm Routing algorithm to generate routable connection IDs.

ServerIdlength Length of serverid to encode/decode server information

refCnt Number of entities using this profile

devno count stateflag

Example

show quicBridge profile

Quicbridge

The entities on which you can perform NetScaler CLI operations:

- quicBridge-profile

rdp

rdp-clientprofile

The following operations can be performed on "rdp-clientprofile":

unset| add| rm| set| show|

unset rdp clientprofile

Use this command to remove rdp clientprofile settings.Refer to the set rdp clientprofile command for meanings of the arguments.

Synopsis

unset rdp clientprofile <name>

add rdp clientprofile

Add an rdp profile.

Synopsis

add rdp clientprofile <name>

Arguments

name The name of the rdp profile

rdpUrlOverride This setting determines whether the RDP parameters supplied in the vpn url override those specified in the RDP profile.

Possible values: ENABLE, DISABLE Default value: ENABLE

redirectClipboard This setting corresponds to the Clipboard check box on the Local Resources tab under Options in RDC.

Possible values: ENABLE, DISABLE Default value: ENABLE

redirectDrives This setting corresponds to the selections for Drives under More on the Local Resources tab under Options in RDC.

Possible values: ENABLE, DISABLE Default value: DISABLE

redirectPrinters This setting corresponds to the selection in the Printers check box on the Local Resources tab under Options in RDC.

Possible values: ENABLE, DISABLE Default value: ENABLE

redirectComPorts This setting corresponds to the selections for comports under More on the Local Resources tab under Options in RDC.

Possible values: ENABLE, DISABLE Default value: DISABLE

redirectPnpDevices This setting corresponds to the selections for pnpdevices under More on the Local Resources tab under Options in RDC.

Possible values: ENABLE, DISABLE Default value: DISABLE

keyboardHook This setting corresponds to the selection in the Keyboard drop-down list on the Local Resources tab under Options in RDC.

Possible values: OnLocal, OnRemote, InFullScreenMode Default value: InFullScreenMode

audioCaptureMode This setting corresponds to the selections in the Remote audio area on the Local Resources tab under Options in RDC.

Possible values: ENABLE, DISABLE Default value: DISABLE

videoPlaybackMode This setting determines if Remote Desktop Connection (RDC) will use RDP efficient multimedia streaming for video playback.

Possible values: ENABLE, DISABLE Default value: ENABLE

multiMonitorSupport Enable/Disable Multiple Monitor Support for Remote Desktop Connection (RDC).

Possible values: ENABLE, DISABLE Default value: ENABLE

rdpCookieValidity RDP cookie validity period. RDP cookie validity time is applicable for new connection and also for any re-connection that might happen, mostly due to network disruption or during fail-over. Default value: 60 Minimum value: 1 Maximum value: 86400

addUserNameInRdpFile Add username in rdp file.

Possible values: YES, NO Default value: NO

rdpFileName RDP file name to be sent to End User

rdpHost Fully-qualified domain name (FQDN) of the RDP Listener.

rdpListener IP address (or) Fully-qualified domain name(FQDN) of the RDP Listener with the port in the format IP:Port (or) FQDN:Port

rdpCustomParams Option for RDP custom parameters settings (if any). Custom params needs to be separated by '&' Default value: 0

psk Pre shared key value Default value: 0

randomizeRDPFilename Will generate unique filename everytime rdp file is downloaded by appending output of time() function in the format <rdpfileName>_<time>.rdp. This tries to avoid the pop-up for replacement of existing rdp file during each rdp connection launch, hence providing better end-user experience.

Possible values: YES, NO Default value: NO

rdpLinkAttribute Citrix Gateway allows the configuration of rdpLinkAttribute parameter which can be used to fetch a list of RDP servers(IP/FQDN) that a user can access, from an Authentication server attribute(Example: LDAP, SAML). Based on the list received, the RDP links will be generated and displayed to the user. Note: The Attribute mentioned in the rdpLinkAttribute should be fetched through corresponding authentication method.

rdpValidateClientIP This setting determines whether RDC launch is initiated by the valid client IP

Possible values: ENABLE, DISABLE Default value: DISABLE

rm rdp clientprofile

Remove an rdp profile

Synopsis

rm rdp clientprofile <name>

Arguments

name The name of the rdp profile.

Example

rm rdp profile

set rdp clientprofile

Modifies the specified parameters for RDP profile.

Synopsis

set rdp clientprofile <name>

Arguments

name The name of the rdp profile

rdpUrlOverride This setting determines whether the RDP parameters supplied in the vpn url override those specified in the RDP profile.

Possible values: ENABLE, DISABLE Default value: ENABLE

redirectClipboard This setting corresponds to the Clipboard check box on the Local Resources tab under Options in RDC.

Possible values: ENABLE, DISABLE Default value: ENABLE

redirectDrives This setting corresponds to the selections for Drives under More on the Local Resources tab under Options in RDC.

Possible values: ENABLE, DISABLE Default value: DISABLE

redirectPrinters This setting corresponds to the selection in the Printers check box on the Local Resources tab under Options in RDC.

Possible values: ENABLE, DISABLE Default value: ENABLE

redirectComPorts This setting corresponds to the selections for comports under More on the Local Resources tab under Options in RDC.

Possible values: ENABLE, DISABLE Default value: DISABLE

redirectPnpDevices This setting corresponds to the selections for pnpdevices under More on the Local Resources tab under Options in RDC.

Possible values: ENABLE, DISABLE Default value: DISABLE

keyboardHook This setting corresponds to the selection in the Keyboard drop-down list on the Local Resources tab under Options in RDC.

Possible values: OnLocal, OnRemote, InFullScreenMode Default value: InFullScreenMode

audioCaptureMode This setting corresponds to the selections in the Remote audio area on the Local Resources tab under Options in RDC.

Possible values: ENABLE, DISABLE Default value: DISABLE

videoPlaybackMode This setting determines if Remote Desktop Connection (RDC) will use RDP efficient multimedia streaming for video playback.

Possible values: ENABLE, DISABLE Default value: ENABLE

multiMonitorSupport Enable/Disable Multiple Monitor Support for Remote Desktop Connection (RDC).

Possible values: ENABLE, DISABLE Default value: ENABLE

rdpCookieValidity RDP cookie validity period. RDP cookie validity time is applicable for new connection and also for any re-connection that might happen, mostly due to network disruption or during fail-over. Default value: 60 Minimum value: 1 Maximum value: 86400

addUserNameInRdpFile Add username in rdp file.

Possible values: YES, NO Default value: NO

rdpFileName RDP file name to be sent to End User

rdpHost Fully-qualified domain name (FQDN) of the RDP Listener.

rdpListener IP address (or) Fully-qualified domain name(FQDN) of the RDP Listener with the port in the format IP:Port (or) FQDN:Port

rdpCustomParams Option for RDP custom parameters settings (if any). Custom params needs to be separated by '&' Default value: 0

psk Pre shared key value Default value: 0

randomizeRDPFilename Will generate unique filename everytime rdp file is downloaded by appending output of time() function in the format <rdpfileName>_<time>.rdp. This tries to avoid the pop-up for replacement of existing rdp file during each rdp connection launch, hence providing better end-user experience.

Possible values: YES, NO Default value: NO

rdpLinkAttribute Citrix Gateway allows the configuration of rdpLinkAttribute parameter which can be used to fetch a list of RDP servers(IP/FQDN) that a user can access, from an Authentication

server attribute(Example: LDAP, SAML). Based on the list received, the RDP links will be generated and displayed to the user. Note: The Attribute mentioned in the rdpLinkAttribute should be fetched through corresponding authentication method.

rdpValidateClientIP This setting determines whether RDC launch is initiated by the valid client IP

Possible values: ENABLE, DISABLE Default value: DISABLE

show rdp clientprofile

Display all rdp profiles

Synopsis

show rdp clientprofile

Arguments

name The name of the rdp profile

Output

rdpUrlOverride This setting determines whether the RDP parameters supplied in the vpn url override those specified in the RDP profile.

redirectClipboard This setting corresponds to the Clipboard check box on the Local Resources tab under Options in RDC.

redirectDrives This setting corresponds to the selections for Drives under More on the Local Resources tab under Options in RDC.

redirectPrinters This setting corresponds to the selection in the Printers check box on the Local Resources tab under Options in RDC.

redirectComPorts This setting corresponds to the selections for comports under More on the Local Resources tab under Options in RDC.

redirectPnpDevices This setting corresponds to the selections for pnpdevices under More on the Local Resources tab under Options in RDC.

keyboardHook This setting corresponds to the selection in the Keyboard drop-down list on the Local Resources tab under Options in RDC.

audioCaptureMode This setting corresponds to the selections in the Remote audio area on the Local Resources tab under Options in RDC.

videoPlaybackMode This setting determines if Remote Desktop Connection (RDC) will use RDP efficient multimedia streaming for video playback.

multiMonitorSupport Enable/Disable Multiple Monitor Support for Remote Desktop Connection (RDC).

rdpCookieValidity RDP cookie validity period. RDP cookie validity time is applicable for new connection and also for any re-connection that might happen, mostly due to network disruption or during fail-over.

addUserNameInRdpFile Add username in rdp file.

rdpFileName RDP file name to be sent to End User

rdpHost Fully-qualified domain name (FQDN) of the RDP Listener.

rdpListener IP address (or) Fully-qualified domain name(FQDN) of the RDP Listener with the port in the format IP:Port (or) FQDN:Port

rdpCustomParams Option for RDP custom parameters settings (if any). Custom params needs to be separated by '&'

psk Pre shared key value

randomizeRDPFilename Will generate unique filename everytime rdp file is downloaded by appending output of time() function in the format <rdpfileName>_<time>.rdp. This tries to avoid the pop-up for replacement of existing rdp file during each rdp connection launch, hence providing better end-user experience.

rdpLinkAttribute Citrix Gateway allows the configuration of rdpLinkAttribute parameter which can be used to fetch a list of RDP servers(IP/FQDN) that a user can access, from an Authentication server attribute(Example: LDAP, SAML). Based on the list received, the RDP links will be generated and displayed to the user. Note: The Attribute mentioned in the rdpLinkAttribute should be fetched through corresponding authentication method.

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

rdpValidateClientIP This setting determines whether RDC launch is initiated by the valid client IP

devno count stateflag

Example

show rdp profile

Rdp

The entities on which you can perform NetScaler CLI operations:

- rdp-clientprofile
- rdp-connections
- rdp-serverprofile

rdp-connections

The following operations can be performed on "rdp-connections":

kill| show|

kill rdp connections

Terminates the specified rdp connections.

Synopsis

kill rdp connections

Arguments

userName User name for which rdp connections needs to be terminated.

all Terminate all active rdpconnections.

Example

kill rdpconnection -username joe

show rdp connections

Displays active connections that use the RDP proxy.

Synopsis

show rdp connections

Arguments

userName User name for which to display connections.

Output

domain The domain name.

endpointIP The client IP address.

endpointPort The client port.

targetIP The Server IP address.

targetPort The server port.

peId Core id of the session owner

stateflag devno count

rdp-serverprofile

The following operations can be performed on "rdp-serverprofile":

add| set| unset| rm| show|

add rdp serverprofile

Add an rdp server profile.

Synopsis

add rdp serverprofile <name> -psk

Arguments

name The name of the rdp server profile

rdpIP IPv4 or IPv6 address of RDP listener. This terminates client RDP connections.

rdpPort TCP port on which the RDP connection is established. Default value: 3389 Minimum value: 1 Maximum value: 65535

psk Pre shared key value

rdpRedirection Enable/Disable RDP redirection support. This needs to be enabled in presence of connection broker or session directory with IP cookie(msts cookie) based redirection support

Possible values: ENABLE, DISABLE Default value: DISABLE

set rdp serverprofile

Modifies the specified parameters for RDP profile.

Synopsis

set rdp serverprofile <name>

Arguments

name The name of the rdp server profile

rdpIP IPv4 or IPv6 address of RDP listener. This terminates client RDP connections.

rdpPort TCP port on which the RDP connection is established. Default value: 3389 Minimum value: 1 Maximum value: 65535

psk Pre shared key value

rdpRedirection Enable/Disable RDP redirection support. This needs to be enabled in presence of connection broker or session directory with IP cookie(msts cookie) based redirection support

Possible values: ENABLE, DISABLE Default value: DISABLE

unset rdp serverprofile

Use this command to remove rdp serverprofile settings.Refer to the set rdp serverprofile command for meanings of the arguments.

Synopsis

unset rdp serverprofile <name>

rm rdp serverprofile

Remove an rdp server profile

Synopsis

rm rdp serverprofile <name>

Arguments

name The name of the rdp server profile.

Example

rm rdp serverprofile

show rdp serverprofile

Display all rdp profiles

Synopsis

show rdp serverprofile

Arguments

name The name of the rdp server profile

Output

rdpIP IPv4 or IPv6 address of RDP listener. This terminates client RDP connections.

rdpPort TCP port on which the RDP connection is established.

psk Pre shared key value

rdpRedirection Enable/Disable RDP redirection support. This needs to be enabled in presence of connection broker or session directory with IP cookie(msts cookie) based redirection support

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

devno count stateflag

Example

show rdp profile

reputationservice

reputation-settings

The following operations can be performed on "reputation-settings":

unset| set| show|

unset reputation settings

Use this command to remove reputation settings settings.Refer to the set reputation settings command for meanings of the arguments.

Synopsis

unset reputation settings

set reputation settings

Sets the reputation service engine settings.

Synopsis

set reputation settings [-proxyUsername <string>]

Arguments

proxyServer Proxy server IP to get Reputation data. Default value: NS_S_REPUTATION_PROXY_SERVER_DEFAULT

proxyPort Proxy server port. Minimum value: 0

proxyUsername Proxy Username

proxyPassword Password with which user logs on.

show reputation settings

Displays the reputation service engine settings.

Synopsis

show reputation settings

Arguments

Output

proxyServer Proxy server IP to get Reputation data.

proxyPort Proxy server port.

proxyUsername Proxy Username

proxyPassword Password with which user logs on.

Reputationservice

The entities on which you can perform NetScaler CLI operations:

- reputation-settings

responder

responder-action

The following operations can be performed on "responder-action":

rename| add| unset| rm| set| show|

rename responder action

Renames a responder action.

Synopsis

rename responder action <name>@ <newName>@

Arguments

name Existing name of the responder action.

newName New name for the responder action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder action" or my responder action').

Example

rename responder action oldname newname

add responder action

Creates a responder action, which specifies how to respond to a request.

Synopsis

add responder action <name> <type> (<target> | <htmlpage>)

Arguments

name Name for the responder action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the responder policy is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder action" or 'my responder action').

type Type of responder action. Available settings function as follows:

- respondwith <target> - Respond to the request with the expression specified as the target.
- respondwithhtmlpage - Respond to the request with the uploaded HTML page object specified as the target.
- redirect - Redirect the request to the URL specified as the target.
- sqlresponse_ok - Send an SQL OK response.
- sqlresponse_error - Send an SQL ERROR response.

Possible values: noop, respondwith, redirect, respondwithhtmlpage, sqlresponse_ok, sqlresponse_error

target Expression specifying what to respond with. Typically a URL for redirect policies or a default-syntax expression. In addition to Citrix ADC default-syntax expressions that refer to information in the request, a stringbuilder expression can contain text and HTML, and simple escape codes that define new lines and paragraphs. Enclose each stringbuilder expression element (either a Citrix ADC default-syntax expression or a string) in double quotation marks. Use the plus (+) character to join the elements.

Examples:

1. Respondwith expression that sends an HTTP 1.1 200 OK response: "HTTP/1.1 200 OK\r\n\r\n"
2. Redirect expression that redirects user to the specified web host and appends the request URL to the redirect. "http://backupsite2.com" + HTTP.REQ.URL
3. Respondwith expression that sends an HTTP 1.1 404 Not Found response with the request URL included in the response: "HTTP/1.1 404 Not Found\r\n\r\n"+ "HTTP.REQ.URL.HTTP_URL_SAFE" + "does not exist on the web server."

The following requirement applies only to the Citrix ADC CLI: Enclose the entire expression in single quotation marks. (Citrix ADC expression elements should be included inside the single quotation marks for the entire expression, but do not need to be enclosed in double quotation marks.)

htmlpage For respondwithhtmlpage policies, name of the HTML page object to use as the response. You must first import the page object.

comment Comment. Any type of information about this responder action.

responseStatusCode HTTP response status code, for example 200, 302, 404, etc. The default value for the redirect action type is 302 and for respondwithhtmlpage is 200 Minimum value: 100 Maximum value: 599

reasonPhrase Expression specifying the reason phrase of the HTTP response. The reason phrase may be a string literal with quotes or a PI expression. For example: "Invalid URL: " + HTTP.REQ.URL

headers One or more headers to insert into the HTTP response. Each header is specified as "name(expr)", where expr is an expression that is evaluated at runtime to provide the value for the named header. You can configure a maximum of eight headers for a responder action.

Example

1. add responder action act1 respondwith "\\"HTTP/1.1 200 OK\\r\\n\\r\\n\\""
2. add responder action resp respondwithhtmlpage my-responder-page,
3. add responder action redir_action redirect "'http://backupsite2.com" + HTTP.REQ.URL'

unset responder action

Use this command to remove responder action settings.Refer to the set responder action command for meanings of the arguments.

Synopsis

unset responder action <name>

rm responder action

Removes the specified responder action.

Synopsis

rm responder action <name>

Arguments

name Name of the responder action to remove.

Example

rm responder action act_before

set responder action

Modifies the specified parameters of a responder action.

Synopsis

set responder action <name>

Arguments

name Name of the responder action to be modified.

target Expression specifying what to respond with. Typically a URL for redirect policies or a default-syntax expression. In addition to Citrix ADC default-syntax expressions that refer to information in the request, a stringbuilder expression can contain text and HTML, and simple escape codes that define new lines and paragraphs. Enclose each stringbuilder expression element (either a Citrix ADC default-syntax expression or a string) in double quotation marks. Use the plus (+) character to join the elements.

Examples:

1. Respondwith expression that sends an HTTP 1.1 200 OK response: "HTTP/1.1 200 OK\r\n\r\n"
2. Redirect expression that redirects user to the specified web host and appends the request URL to the redirect. "http://backupsite2.com" + HTTP.REQ.URL
3. Respondwith expression that sends an HTTP 1.1 404 Not Found response with the request URL included in the response: "HTTP/1.1 404 Not Found\r\n\r\n"+ "HTTP.REQ.URL.HTTP_URL_SAFE" + "does not exist on the web server."

The following requirement applies only to the Citrix ADC CLI: Enclose the entire expression in single quotation marks. (Citrix ADC expression elements should be included inside the single

quotation marks for the entire expression, but do not need to be enclosed in double quotation marks.)

htmlpage For respondwithhtmlpage policies, name of the HTML page object to use as the response. You must first import the page object.

responseStatusCode HTTP response status code, for example 200, 302, 404, etc. The default value for the redirect action type is 302 and for respondwithhtmlpage is 200 Minimum value: 100 Maximum value: 599

reasonPhrase Expression specifying the reason phrase of the HTTP response. The reason phrase may be a string literal with quotes or a PI expression. For example: "Invalid URL: " + HTTP.REQ.URL

comment Comment. Any type of information about this responder action.

headers One or more headers to insert into the HTTP response. Each header is specified as "name(expr)", where expr is an expression that is evaluated at runtime to provide the value for the named header. You can configure a maximum of eight headers for a responder action.

Example

1. set responder action act_responder -target 'HTTP.REQ.HEADER(MYURL) -redirectresponsecode <respcode>'/,
2. set responder action act_responder -htmlpage my-local-file

show responder action

Displays the current settings for the specified responder action. If no action name is provided, displays a list of all responder actions currently configured on the Citrix ADC, with abbreviated settings.

Synopsis

show responder action

Arguments

name Name of the responder action.

Output

stateflag type Type of responder action. It can be: (respondwith).

target Expression specifying what to to respond with

htmlpage Option specifying to respondwith htmlpage

bypassSafetyCheck The safety check to allow unsafe expressions.

hits The number of times the action has been taken.

referenceCount The number of references to the action.

undefHits The number of times the action resulted in UNDEF.

comment Comment. Any type of information about this responder action.

builtin Flag to determine whether responder action is built-in or not

feature The feature to be checked while applying this config

responseStatusCode HTTP response status code, for example 200, 302, 404, etc. The default value for the redirect action type is 302 and for respondwithhtmlpage is 200

reasonPhrase Expression specifying the reason phrase of the HTTP response. The reason phrase may be a string literal with quotes or a PI expression. For example: "Invalid URL: " + HTTP.REQ.URL

headers One or more headers to insert into the HTTP response. Each header is specified as "name(expr)", where expr is an expression that is evaluated at runtime to provide the value for the named header. You can configure a maximum of eight headers for a responder action.

devno count

Example

1. show responder action
2. show responder action act_insert

Responder

The entities on which you can perform NetScaler CLI operations:

- responder-action
- responder-global
- responder-htmlpage

- responder-param
- responder-policy
- responder-policylabel

responder-global

The following operations can be performed on "responder-global":

unbind| bind| show|

unbind responder global

Unbind the specified responder policy from responder global.

Synopsis

unbind responder global <policyName>

Arguments

policyName Name of the policy to unbind.

type The bindpoint from which the policy is to be unbound.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, OVERRIDE, DEFAULT, OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, SIPUDP_REQ_OVERRIDE, SIPUDP_REQ_DEFAULT, SIPTCP_REQ_OVERRIDE, SIPTCP_REQ_DEFAULT, MSSQL_REQ_OVERRIDE, MSSQL_REQ_DEFAULT, MYSQL_REQ_OVERRIDE, MYSQL_REQ_DEFAULT, NAT_REQ_OVERRIDE, NAT_REQ_DEFAULT, DIAMETER_REQ_OVERRIDE, DIAMETER_REQ_DEFAULT, RADIUS_REQ_OVERRIDE, RADIUS_REQ_DEFAULT, DNS_REQ_OVERRIDE, DNS_REQ_DEFAULT, MQTT_REQ_OVERRIDE, MQTT_REQ_DEFAULT, MQTT_JUMBO_REQ_OVERRIDE, MQTT_JUMBO_REQ_DEFAULT, QUIC_OVERRIDE, QUIC_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT

priority Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind responder global pol9

bind responder global

Activates the specified responder policy for all requests sent to the Citrix ADC.

Synopsis

bind responder global <policyName> <priority>

Arguments

policyName Name of the responder policy to activate. If you want to create the policy as well as activate it, specify a name for the responder policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder policy" or 'my responder policy').

priority Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Must be unique within the label. Policies are evaluated in the order of their priority numbers, and the first policy that matches the request is applied. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.
- The expression evaluates to a priority number that is smaller than the current policy's priority number.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

type Bind point to which to bind the policy. Available settings function as follows:

- REQ_OVERRIDE - Request override. Binds the policy to the priority request queue.
- REQ_DEFAULT - Binds the policy to the default request queue.
- OTHERTCP_REQ_OVERRIDE - Binds the policy to the non-HTTP TCP priority request queue.
- OTHERTCP_REQ_DEFAULT - Binds the policy to the non-HTTP TCP default request queue.
- SIPUDP_REQ_OVERRIDE - Binds the policy to the SIP UDP priority response queue.
- SIPUDP_REQ_DEFAULT - Binds the policy to the SIP UDP default response queue.
- RADIUS_REQ_OVERRIDE - Binds the policy to the RADIUS priority response queue.
- RADIUS_REQ_DEFAULT - Binds the policy to the RADIUS default response queue.
- MSSQL_REQ_OVERRIDE - Binds the policy to the Microsoft SQL priority response queue.
- MSSQL_REQ_DEFAULT - Binds the policy to the Microsoft SQL default response queue.
- MYSQL_REQ_OVERRIDE - Binds the policy to the MySQL priority response queue.
- MYSQL_REQ_DEFAULT - Binds the policy to the MySQL default response queue.
- NAT_REQ_OVERRIDE - Binds the policy to the NAT priority request queue.
- NAT_REQ_DEFAULT - Binds the policy to the NAT default request queue.
- MQTT_REQ_OVERRIDE - Binds the policy to the MQTT priority queue.
- MQTT_REQ_DEFAULT - Binds the policy to the MQTT default queue.
- MQTT_JUMBO_REQ_OVERRIDE - Binds the policy to the MQTT Jumo priority queue.
- MQTT_JUMBO_REQ_DEFAULT - Binds the policy to the MQTT Jumbo default queue.
- HTTPQUIC_REQ_OVERRIDE - Binds the policy to the HTTP_QUIC override queue.
- HTTPQUIC_REQ_DEFAULT - Binds the policy to the HTTP_QUIC default queue.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, OVERRIDE, DEFAULT, OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, SIPUDP_REQ_OVERRIDE, SIPUDP_REQ_DEFAULT, SIPTCP_REQ_OVERRIDE, SIPTCP_REQ_DEFAULT, MSSQL_REQ_OVERRIDE, MSSQL_REQ_DEFAULT, MYSQL_REQ_OVERRIDE, MYSQL_REQ_DEFAULT, NAT_REQ_OVERRIDE, NAT_REQ_DEFAULT, DIAMETER_REQ_OVERRIDE, DIAMETER_REQ_DEFAULT, RADIUS_REQ_OVERRIDE, RADIUS_REQ_DEFAULT, DNS_REQ_OVERRIDE, DNS_REQ_DEFAULT, MQTT_REQ_OVERRIDE, MQTT_REQ_DEFAULT, MQTT_JUMBO_REQ_OVERRIDE, MQTT_JUMBO_REQ_DEFAULT, QUIC_OVERRIDE, QUIC_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

labelType Type of invocation, Available settings function as follows:

- vserver - Forward the request to the specified virtual server.
- policylabel - Invoke the specified policy label.

Possible values: vserver, policylabel

labelName Name of the policy label to invoke. If the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is policylabel.

Example

i)bind responder global pol9 9

show responder global

Displays the list of policies bound to the specified responder global bind point. If no bind point is specified, displays a list of all policies bound to responder global.

Synopsis

show responder global

Arguments

type Specifies the bind point whose policies you want to display. Available settings function as follows:

- REQ_OVERRIDE - Request override. Binds the policy to the priority request queue.
- REQ_DEFAULT - Binds the policy to the default request queue.
- OTHERTCP_REQ_OVERRIDE - Binds the policy to the non-HTTP TCP priority request queue.
- OTHERTCP_REQ_DEFAULT - Binds the policy to the non-HTTP TCP default request queue..
- SIPUDP_REQ_OVERRIDE - Binds the policy to the SIP UDP priority response queue..
- SIPUDP_REQ_DEFAULT - Binds the policy to the SIP UDP default response queue.
- RADIUS_REQ_OVERRIDE - Binds the policy to the RADIUS priority response queue..
- RADIUS_REQ_DEFAULT - Binds the policy to the RADIUS default response queue.
- MSSQL_REQ_OVERRIDE - Binds the policy to the Microsoft SQL priority response queue..
- MSSQL_REQ_DEFAULT - Binds the policy to the Microsoft SQL default response queue.
- MYSQL_REQ_OVERRIDE - Binds the policy to the MySQL priority response queue.
- MYSQL_REQ_DEFAULT - Binds the policy to the MySQL default response queue.
- HTTPQUIC_REQ_OVERRIDE - Binds the policy to the HTTP_QUIC override response queue.
- HTTPQUIC_REQ_DEFAULT - Binds the policy to the HTTP_QUIC default response queue.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, OVERRIDE, DEFAULT, OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, SIPUDP_REQ_OVERRIDE, SIPUDP_REQ_DEFAULT, SIPTCP_REQ_OVERRIDE, SIPTCP_REQ_DEFAULT, MSSQL_REQ_OVERRIDE, MSSQL_REQ_DEFAULT, MYSQL_REQ_OVERRIDE, MYSQL_REQ_DEFAULT, NAT_REQ_OVERRIDE, NAT_REQ_DEFAULT, DIAMETER_REQ_OVERRIDE, DIAMETER_REQ_DEFAULT, RADIUS_REQ_OVERRIDE, RADIUS_REQ_DEFAULT, DNS_REQ_OVERRIDE, DNS_REQ_DEFAULT, MQTT_REQ_OVERRIDE, MQTT_REQ_DEFAULT, MQTT_JUMBO_REQ_OVERRIDE, MQTT_JUMBO_REQ_DEFAULT, QUIC_OVERRIDE, QUIC_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT

Output

stateflag policyName Name of the responder policy.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

labelType Type of invocation, Available settings function as follows:

- vserver - Forward the request to the specified virtual server.
- policylabel - Invoke the specified policy label.

labelName Name of the policy label to invoke. If the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is policylabel.

flowType flowtype of the bound responder policy.

numpol number of polices bound to label.

flags globalBindType devno count

Example

show responder global

responder-htmlpage

The following operations can be performed on "responder-htmlpage":

show| update| import| rm|

show responder htmlpage

Displays the specified HTML page object. If no HTML page object is specified, lists all HTML page objects on the Citrix ADC.

Synopsis

show responder htmlpage

Arguments

name Name of the HTML page object to display.

Output

response

Example

show responder htmlpage

update responder htmlpage

Updates the specified HTML page object from the source.

Synopsis

update responder htmlpage <name>

Arguments

name Name to assign to the HTML page object on the Citrix ADC.

Example

update responder htmlpage my-responder-page

import responder htmlpage

Imports the specified HTML page to the Citrix ADC, assigns it the specified name, and stores it in the list of Responder HTML page objects. This page can be used as a HTTP response body using the Responder respondwithhtmlpage action type. The HTML page can contain expressions and the maximum number of expressions allowed is 1000.

Synopsis

import responder htmlpage <name>

Arguments

src Local path or URL (protocol, host, path, and file name) for the file from which to retrieve the imported HTML page. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

name Name to assign to the HTML page object on the Citrix ADC.

comment Any comments to preserve information about the HTML page object.

overwrite Overwrites the existing file

CAcertFile CA certificate file name which will be used to verify the peer's certificate. The certificate should be imported using "import ssl certfile" CLI command or equivalent in API or GUI. If

certificate name is not configured, then default root CA certificates are used for peer's certificate verification.

Example

import responder htmlpage http://www.example.com/page.html my-responder-page

rm responder htmlpage

Removes the specified HTML page object.

Synopsis

rm responder htmlpage <name>

Arguments

name Name of the HTML page object to remove.

Example

rm responder htmlpage <name>

responder-param

The following operations can be performed on "responder-param":

unset| set| show|

unset responder param

Use this command to remove responder param settings.Refer to the set responder param command for meanings of the arguments.

Synopsis

unset responder param

set responder param

Sets the given Responder parameter(s).

Synopsis

set responder param

Arguments

undefAction Action to perform when policy evaluation creates an UNDEF condition. Available settings function as follows:

- NOOP - Send the request to the protected server.
- RESET - Reset the request and notify the user's browser, so that the user can resend the request.
- DROP - Drop the request without sending a response to the user. Default value: "NOOP"

timeout Maximum time in milliseconds to allow for processing all the policies and their selected actions without interruption. If the timeout is reached then the evaluation causes an UNDEF to be raised and no further processing is performed. Default value: 3900 Minimum value: 1 Maximum value: 5000

Example

set responder param -undefAction RESET -timeout 3000

show responder param

Displays the Responder parameters.

Synopsis

show responder param

Arguments

Output

undefAction Name of the responder action.

timeout Maximum time in milliseconds to allow for processing all the policies and their selected actions without interruption. If the timeout is reached then the evaluation causes an UNDEF to be raised and no further processing is performed.

Example

show responder param

responder-policy

The following operations can be performed on "responder-policy":

rm| stat| show| rename| unset| set| add|

rm responder policy

Removes the specified responder policy.

Synopsis

rm responder policy <name>

Arguments

name Name of the responder policy to remove.

Example

rm responder policy pol9

stat responder policy

Displays statistics for all responder policies currently configured on the Citrix ADC, or detailed statistics for the specified policy.

Synopsis

stat responder policy

Arguments

name Name of the responder policy for which to show detailed statistics.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Policy undef hits (Undefhits) Number of undef hits on the policy

Related Commands

- stat responder policylabel

show responder policy

Displays the current settings for the specified responder policy. If no policy name is specified, displays a list of all responder policies currently configured on the Citrix ADC, with abbreviated settings.

Synopsis

show responder policy show responder policy stats - alias for 'stat responder policy'

Arguments

name Name of the responder policy for which to display settings.

Output

stateflag rule Rule of the policy.

action Responder action associated with the policy.

undefAction UNDEF action associated with the policy.

hits Number of hits.

undefHits Number of policy UNDEF hits.

activePolicy Indicates whether policy is bound or not.

boundTo Location where policy is bound

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

comment Any type of information about this responder policy.

logAction Name of the messagelog action to use for requests that match this policy.

bindPolicyType vserverType appflowAction AppFlow action to invoke for requests that match this policy.

builtin Flag to determine if responder policy is built-in or not

feature The feature to be checked while applying this config

type devno count

Example

show responder policy

rename responder policy

Renames the specified responder policy.

Synopsis

rename responder policy <name>@ <newName>@

Arguments

name Existing name of the responder policy.

newName New name for the responder policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder policy" or 'my responder policy').

Example

rename responder policy oldname newname

unset responder policy

Removes the settings of an existing responder policy. Attributes for which a default value is available revert to their default values. See the set responder policy command for descriptions of the parameters..Refer to the set responder policy command for meanings of the arguments.

Synopsis

unset responder policy <name>

Example

unset responder policy respol9 -undefAction

set responder policy

Modifies the rule or action portion of the specified responder policy.

Synopsis

set responder policy <name>

Arguments

name Name of the responder policy.

rule Expression that the policy uses to determine whether to respond to the specified request.

action Name of the responder action to perform if the request matches this responder policy. There are also some built-in actions which can be used. These are:

- NOOP - Send the request to the protected server instead of responding to it.
- RESET - Reset the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend the request if desired.
- DROP - Drop the request without sending a response to the user.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

comment Any type of information about this responder policy.

logAction Name of the messagelog action to use for requests that match this policy.

appflowAction AppFlow action to invoke for requests that match this policy.

Example

set responder policy pol9 -rule "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh2\\")"

add responder policy

Creates a responder policy, which specifies requests that the Citrix ADC intercepts and responds to directly instead of forwarding them to a protected server.

Synopsis

add responder policy <name> <rule> <action>

Arguments

name Name for the responder policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the responder policy is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder policy" or 'my responder policy').

rule Expression that the policy uses to determine whether to respond to the specified request.

action Name of the responder action to perform if the request matches this responder policy. There are also some built-in actions which can be used. These are:

- NOOP - Send the request to the protected server instead of responding to it.
- RESET - Reset the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend the request if desired.
- DROP - Drop the request without sending a response to the user.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

comment Any type of information about this responder policy.

logAction Name of the messagelog action to use for requests that match this policy.

appflowAction AppFlow action to invoke for requests that match this policy.

Example

i) add responder policy pol9 "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh3\\")" act_respondwith

responder-policylabel

The following operations can be performed on "responder-policylabel":

show| unbind| rm| add| stat| bind| rename|

show responder policylabel

Displays the current settings for the specified responder policy label. If no policy label is specified, displays a list of all responder policy labels currently configured on the Citrix ADC, with abbreviated settings.

Synopsis

show responder policylabel

Arguments

labelName Name of the responder policy label.

Output

policylabeltype The type of the policy label.

stateflag numpol number of polices bound to label.

hits Number of times policy label was invoked.

policyName Name of the responder policy.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label and evaluate the specified policy label.

labelType Type of policy label to invoke. Available settings function as follows:

- vserver - Invoke an unnamed policy label associated with a virtual server.

- policylabel - Invoke a user-defined policy label.

labelName

- If labelType is policylabel, name of the policy label to invoke.
- If labelType is reqvserver or resvserver, name of the virtual server.

flags comment Any comments to preserve information about this responder policy label.

devno count

Example

i)show responder policylabel resp_lab ii)show responder policylabel

unbind responder policylabel

Unbinds the specified responder policy from the specified policy label.

Synopsis

unbind responder policylabel <labelName> <policyName>

Arguments

labelName Name for the responder policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the responder policy label is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder policy label" or my responder policy label').

policyName The name of the policy to be unbound.

priority Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind responder policylabel resp_lab pol_resp

rm responder policylabel

Removes a responder policy label.

Synopsis

rm responder policylabel <labelName>

Arguments

labelName Name of the responder policy label to remove.

Example

rm responder policylabel resp_lab

add responder policylabel

Creates a user-defined responder policy label, to which you can bind policies. A policy label is a tool for evaluating a set of policies in a specified order. By using a policy label, you can configure the responder feature to choose the next policy, invoke a different policy label, or terminate policy evaluation completely by looking at whether the previous policy evaluated to TRUE or FALSE.

Synopsis

add responder policylabel <labelName>

Arguments

labelName Name for the responder policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the responder policy label is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder policy label" or my responder policy label').

policylabeltype Type of responses sent by the policies bound to this policy label. Types are:

- HTTP - HTTP responses.
- OTHERTCP - NON-HTTP TCP responses.
- SIP_UDP - SIP responses.
- RADIUS - RADIUS responses.
- MYSQL - SQL responses in MySQL format.
- MSSQL - SQL responses in Microsoft SQL format.

- NAT - NAT response.
- MQTT - Trigger policies bind with MQTT type.
- MQTT_JUMBO - Trigger policies bind with MQTT Jumbo type.

Possible values: HTTP, OTHERTCP, SIP_UDP, SIP_TCP, MYSQL, MSSQL, NAT, DIAMETER, RADIUS, DNS, MQTT, MQTT_JUMBO, QUIC_BRIDGE, HTTP_QUIC Default value: HTTP

comment Any comments to preserve information about this responder policy label.

Example

add responder policylabel resp_lab

stat responder policylabel

Displays statistics for the specified responder policy label. If no policy label name is provided, displays abbreviated statistics for all responder policy labels currently configured on the Citrix ADC.

Synopsis

stat responder policylabel

Arguments

labelName Name of the responder policy label.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy Label Hits (Hits) Number of times policy label was invoked.

bind responder policylabel

Binds the specified responder policy to the specified policy label.

Synopsis

bind responder policylabel <labelName> <policyName> <priority>

Arguments

labelName Name of the responder policy label to which to bind the policy.

policyName Name of the policy to bind to the responder policy label.

priority Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Must be unique within the label. Policies are evaluated in the order of their priority numbers, and the first policy that matches the request is applied. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.
- The expression evaluates to a priority number that is smaller than the current policys priority number.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label and evaluate the specified policy label.

labelType Type of policy label to invoke. Available settings function as follows:

- vserver - Invoke an unnamed policy label associated with a virtual server.
- policylabel - Invoke a user-defined policy label.

Possible values: vserver, policylabel

labelName

- If labelType is policylabel, name of the policy label to invoke.
- If labelType is reqvserver or resvserver, name of the virtual server.

Example

i)bind responder policylabel resp_lab pol_resp 1 2 ii)bind responder policylabel resp_lab pol_resp 1 2 -invoke vserver CURRENT

rename responder policylabel

Renames the specified responder policy label.

Synopsis

rename responder policylabel <labelName>@ <newName>@

Arguments

labelName Current name of the responder policy label.

newName New name for the responder policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

Example

rename responder policylabel oldname newname

rewrite

rewrite-action

The following operations can be performed on "rewrite-action":

rename| show| set| add| rm| unset|

rename rewrite action

Renames a rewrite action.

Synopsis

rename rewrite action <name>@ <newName>@

Arguments

name Existing name of the rewrite action.

newName New name for the rewrite action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the rewrite policy is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my rewrite action" or 'my rewrite action').

Example

rename rewrite action oldname newname

show rewrite action

Displays the current settings for the specified rewrite action. If no rewrite action name is provided, displays a list of all rewrite actions currently configured on the Citrix ADC.

Synopsis

show rewrite action

Arguments

name Name of the rewrite action.

Output

stateflag type Type of rewrite action. It can be: (delete|replace|insert_http_header|insert_before|insert_after|replace_http_res).

target Expression specifying which part of HTTP header needs to be rewritten.

stringBuilderExpr Expression specifying the value of rewritten HTTP header.

search Search facility that is used to match multiple strings in the request or response. Used in the INSERT_BEFORE_ALL, INSERT_AFTER_ALL, REPLACE_ALL, and DELETE_ALL action types. The following search types are supported:

- Text ("text(string)") - A literal string. Example: -search text("hello")
- Regular expression ("regex(re<delimiter>regular exp<delimiter>)") - Pattern that is used to match multiple strings in the request or response. The pattern may be a PCRE-format regular expression with a delimiter that consists of any printable ASCII non-alphanumeric character except for the underscore (_) and space ( ) that is not otherwise used in the expression. Example: -search regex(re~\^hello*~) The preceding regular expression can use the tilde (~) as the delimiter because that character does not appear in the regular expression itself.
- XPath ("xpath(xp<delimiter>xpath expression<delimiter>)") - An XPath expression to search XML. The delimiter has the same rules as for regex. Example: -search xpath(xp%/a/b%)
- JSON ("xpath_json(xp<delimiter>xpath expression<delimiter>)") - An XPath expression to search JSON. The delimiter has the same rules as for regex. Example: -search xpath_json(xp%/a/b%) NOTE: JSON searches use the same syntax as XPath searches, but operate on JSON files instead of standard XML files.
- HTML ("xpath_html(xp<delimiter>xpath expression<delimiter>)") - An XPath expression to search HTML. The delimiter has the same rules as for regex. Example: -search xpath_html(xp%/html/body%) NOTE: HTML searches use the same syntax as XPath searches, but operate on HTML files instead of standard XML files; HTML 5 rules for the file syntax are used; HTML 4 and later are supported.
- Patset ("patset(patset)") - A predefined pattern set. Example: -search patset("patset1").
- Datset ("dataset(dataset)") - A predefined dataset. Example: -search dataset("dataset1").
- AVP ("avp(avp number)") - AVP number that is used to match multiple AVPs in a Diameter/Radius Message. Example: -search avp(999)

Note: for all these the TARGET prefix can be used in the replacement expression to specify the text that was selected by the -search parameter, optionally adjusted by the -refineSearch parameter. Example: TARGET.BEFORE_STR(",")

refineSearch Specify additional criteria to refine the results of the search. Always starts with the "extend(m,n)" operation, where 'm' specifies number of bytes to the left of selected data and 'n' specifies number of bytes to the right of selected data to extend the selected area. You can use refineSearch only on body expressions, and for the INSERT_BEFORE_ALL, INSERT_AFTER_ALL, REPLACE_ALL, and DELETE_ALL action types. Example: -refineSearch 'EXTEND(10, 20).REGEX_SELECT(re~0x+~).

hits The number of times the action has been taken.

undefHits The number of times the action resulted in UNDEF.

referenceCount The number of references to the action.

description Description of the action

flags isDefault A value of true is returned if it is a default rewriteaction.

comment Comment. Can be used to preserve information about this rewrite action.

builtin Flag to determine whether rewrite action is built-in or not

feature The feature to be checked while applying this config

devno count

Example

1. show rewrite action
2. show rewrite action act_insert

set rewrite action

Modifies the specified parameters of a rewrite action.

Synopsis

set rewrite action <name>

Arguments

name Name of the rewrite action to modify.

target Expression that specifies which part of the connection to rewrite.

stringBuilderExpr Expression that specifies the content to insert into the request or response at the specified location, or that replaces the specified string.

search Search facility that is used to match multiple strings in the request or response. Used in the INSERT_BEFORE_ALL, INSERT_AFTER_ALL, REPLACE_ALL, and DELETE_ALL action types. The following search types are supported:

- Text ("text(string)") - A literal string. Example: -search text("hello")
- Regular expression ("regex(re<delimiter>regular exp<delimiter>)") - Pattern that is used to match multiple strings in the request or response. The pattern may be a PCRE-format regular expression with a delimiter that consists of any printable ASCII non-alphanumeric character except for the underscore (_) and space ( ) that is not otherwise used in the expression. Example: -search regex(re~\^hello*~) The preceding regular expression can use the tilde (~) as the delimiter because that character does not appear in the regular expression itself.
- XPath ("xpath(xp<delimiter>xpath expression<delimiter>)") - An XPath expression to search XML. The delimiter has the same rules as for regex. Example: -search xpath(xp%/a/b%)
- JSON ("xpath_json(xp<delimiter>xpath expression<delimiter>)") - An XPath expression to search JSON. The delimiter has the same rules as for regex. Example: -search xpath_json(xp%/a/b%) NOTE: JSON searches use the same syntax as XPath searches, but operate on JSON files instead of standard XML files.
- HTML ("xpath_html(xp<delimiter>xpath expression<delimiter>)") - An XPath expression to search HTML. The delimiter has the same rules as for regex. Example: -search xpath_html(xp%/html/body%) NOTE: HTML searches use the same syntax as XPath searches, but operate on HTML files instead of standard XML files; HTML 5 rules for the file syntax are used; HTML 4 and later are supported.
- Patset ("patset(patset)") - A predefined pattern set. Example: -search patset("patset1").
- Datset ("dataset(dataset)") - A predefined dataset. Example: -search dataset("dataset1").
- AVP ("avp(avp number)") - AVP number that is used to match multiple AVPs in a Diameter/ Radius Message. Example: -search avp(999)

Note: for all these the TARGET prefix can be used in the replacement expression to specify the text that was selected by the -search parameter, optionally adjusted by the -refineSearch parameter. Example: TARGET.BEFORE_STR(",")

refineSearch Specify additional criteria to refine the results of the search. Always starts with the "extend(m,n)" operation, where 'm' specifies number of bytes to the left of selected data and 'n' specifies number of bytes to the right of selected data to extend the selected area. You can use refineSearch only on body expressions, and for the INSERT_BEFORE_ALL, INSERT_AFTER_ALL, REPLACE_ALL, and DELETE_ALL action types. Example: -refineSearch 'EXTEND(10, 20).REGEX_SELECT(re~0x+~).

comment Comment. Can be used to preserve information about this rewrite action.

Example

set rewrite action rwact1 -target "HTTP.REQ.HEADER(\\"MyHdr\\")" -stringBuilderExpr "HTTP.REQ.URL.MARK_SAFE"

add rewrite action

Creates a rewrite action, which specifies exactly what modifications to make to a request or response before forwarding that request or response to the protected web server or to the user. In addition to user-defined actions, the rewrite feature has the following three built-in actions:

- NOREWRITE - Sends the request or response to the user without rewriting it.
- RESET - Resets the connection and notifies the user's browser, so that the user can resend the request.
- DROP - Drops the connection without sending a response to the user. One of the following three flow types is implicitly associated with every action:
- Request - Action applies to the request.
- Response - Action applies to the response.
- Neutral - Action applies to both requests and responses.

Synopsis

add rewrite action <name> <type> <target>

Arguments

name Name for the user-defined rewrite action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the rewrite policy is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my rewrite action" or 'my rewrite action').

type Type of user-defined rewrite action. The information that you provide for, and the effect of, each type are as follows::

- REPLACE <target> <string_builder_expr>. Replaces the string with the string-builder expression.
- REPLACE_ALL <target> <string_builder_expr> -search <search_expr>. In the request or response specified by <target>, replaces all occurrences of the string defined by <string_builder_expr> with the string defined by <search_expr>.
- REPLACE_HTTP_RES <string_builder_expr>. Replaces the complete HTTP response with the string defined by the string-builder expression.
- REPLACE_SIP_RES <target> - Replaces the complete SIP response with the string specified by <target>.
- INSERT_HTTP_HEADER <header_string_builder_expr> <contents_string_builder_expr>. Inserts the HTTP header specified by <header_string_builder_expr> and header contents specified by <contents_string_builder_expr>.
- DELETE_HTTP_HEADER <target>. Deletes the HTTP header specified by <target>.
- CORRUPT_HTTP_HEADER <target>. Replaces the header name of all occurrences of the HTTP header specified by <target> with a corrupted name, so that it will not be recognized by the receiver Example: MY_HEADER is changed to MHEY_ADER.
- INSERT_BEFORE <target_expr> <string_builder_expr>. Finds the string specified in <target_expr> and inserts the string in <string_builder_expr> before it.
- INSERT_BEFORE_ALL <target> <string_builder_expr> -search <search_expr>. In the request or response specified by <target>, locates all occurrences of the string specified in <string_builder_expr> and inserts the string specified in <search_expr> before each.
- INSERT_AFTER <target_expr> <string_builder_expr>. Finds the string specified in <target_expr>, and inserts the string specified in <string_builder_expr> after it.
- INSERT_AFTER_ALL <target> <string_builder_expr> -search <search_expr>. In the request or response specified by <target>, locates all occurrences of the string specified by <string_builder_expr> and inserts the string specified by <search_expr> after each.
- DELETE <target>. Finds and deletes the specified target.

- DELETE_ALL <target> -search <string_builder_expr>. In the request or response specified by <target>, locates and deletes all occurrences of the string specified by <string_builder_expr>.
- REPLACE_DIAMETER_HEADER_FIELD <target> <field value>. In the request or response modify the header field specified by <target>. Use Diameter.req.flags.SET(<flag>) or Diameter.req.flags.UNSET<flag> as 'stringbuilderexpression' to set or unset flags.
- REPLACE_DNS_HEADER_FIELD <target>. In the request or response modify the header field specified by <target>.
- REPLACE_DNS_ANSWER_SECTION <target>. Replace the DNS answer section in the response. This is currently applicable for A and AAAA records only. Use DNS.NEW_RRSET_A & DNS.NEW_RRSET_AAAA expressions to configure the new answer section.
- REPLACE_MQTT <target> <string_builder_expr> : Replace MQTT message fields specified in <target_expr> to the value specified in <string_builder_expr>
- INSERT_MQTT <string_builder_expr> : Insert the string_builder_expr to an appropriate packet field in the MQTT message.
- INSERT_AFTER_MQTT <target_expr> <string_builder_expr> : Insert a topic specified in <string_builder_expr> in the MQTT Subscribe or Unsubscribe message after the specified target_expr.
- INSERT_BEFORE_MQTT <target_expr> <string_builder_expr> : Insert a topic specified in <string_builder_expr> in the MQTT Subscribe or Unsubscribe message before the specified target_expr.
- DELETE_MQTT <target> : Deletes the specified target in the MQTT message.

Possible values: noop, delete, insert_http_header, delete_http_header, corrupt_http_header, insert_before, insert_after, replace, replace_http_res, delete_all, replace_all, insert_before_all, insert_after_all, clientless_vpn_encode, clientless_vpn_encode_all, clientless_vpn_decode, clientless_vpn_decode_all, insert_sip_header, delete_sip_header, corrupt_sip_header, replace_sip_res, replace_diameter_header_field, replace_dns_header_field, replace_dns_answer_section, replace_mqtt, delete_mqtt, insert_mqtt, insert_before_mqtt, insert_after_mqtt

target Expression that specifies which part of the request or response to rewrite.

stringBuilderExpr Expression that specifies the content to insert into the request or response at the specified location, or that replaces the specified string.

search Search facility that is used to match multiple strings in the request or response. Used in the INSERT_BEFORE_ALL, INSERT_AFTER_ALL, REPLACE_ALL, and DELETE_ALL action types. The following search types are supported:

- Text ("text(string)") - A literal string. Example: -search text("hello")
- Regular expression ("regex(re<delimiter>regular exp<delimiter>)") - Pattern that is used to match multiple strings in the request or response. The pattern may be a PCRE-format regular expression with a delimiter that consists of any printable ASCII non-alphanumeric character except for the underscore (_) and space ( ) that is not otherwise used in the expression. Example: -search regex(re~\^hello*~) The preceding regular expression can use the tilde (~) as the delimiter because that character does not appear in the regular expression itself.
- XPath ("xpath(xp<delimiter>xpath expression<delimiter>)") - An XPath expression to search XML. The delimiter has the same rules as for regex. Example: -search xpath(xp%/a/b%)
- JSON ("xpath_json(xp<delimiter>xpath expression<delimiter>)") - An XPath expression to search JSON. The delimiter has the same rules as for regex. Example: -search xpath_json(xp%/a/b%) NOTE: JSON searches use the same syntax as XPath searches, but operate on JSON files instead of standard XML files.
- HTML ("xpath_html(xp<delimiter>xpath expression<delimiter>)") - An XPath expression to search HTML. The delimiter has the same rules as for regex. Example: -search xpath_html(xp%/html/body%) NOTE: HTML searches use the same syntax as XPath searches, but operate on HTML files instead of standard XML files; HTML 5 rules for the file syntax are used; HTML 4 and later are supported.
- Patset ("patset(patset)") - A predefined pattern set. Example: -search patset("patset1").
- Datset ("dataset(dataset)") - A predefined dataset. Example: -search dataset("dataset1").
- AVP ("avp(avp number)") - AVP number that is used to match multiple AVPs in a Diameter/ Radius Message. Example: -search avp(999)

Note: for all these the TARGET prefix can be used in the replacement expression to specify the text that was selected by the -search parameter, optionally adjusted by the -refineSearch parameter. Example: TARGET.BEFORE_STR(",")

refineSearch Specify additional criteria to refine the results of the search. Always starts with the "extend(m,n)" operation, where 'm' specifies number of bytes to the left of selected data and 'n' specifies number of bytes to the right of selected data to extend the selected area. You can use refineSearch only on body expressions, and for the INSERT_BEFORE_ALL,

INSERT_AFTER_ALL, REPLACE_ALL, and DELETE_ALL action types. Example: -refineSearch 'EXTEND(10, 20).REGEX_SELECT(re~0x+~).

comment Comment. Can be used to preserve information about this rewrite action.

Example

i)add rewrite action act_insert INSERT_HTTP_HEADER change_req "\\"no change\\"" .This Adds to http header will add the header change_req: no change. ii)add rewrite action act_replace REPLACE "HTTP.REQ.URL.PREFIX(1)" "HTTP.REQ.URL.PREFIX(1)+\\"citrix/\\"" .If HTTP.REQ.URL.PREFIX(1) is / the result would be /citrix/ iii)add rewrite action act_before INSERT_BEFORE "HTTP.REQ.HEADER(\\"host\\").VALUE(0)" "\\"india\\"" .If HTTP.REQ.HEADER(\\"host\\").VALUE(0) is netscaler.com the result would be indianetscaler.com iv)add rewrite action act_after INSERT_AFTER "HTTP.REQ.HEADER(\\"host\ \").TYPECAST_LIST_T('.').GET(0)" "\\"-india\\"" .If HTTP.REQ.HEADER(\\"host\\").VALUE(0) is support.netscaler.com then the result would be support-india.netscaler.com v)add rewrite action act_delete DELETE "HTTP.REQ.HEADER(\\"host\\").VALUE(0)" will leave the Host header looking like "HOST: ". vi)add rewrite action act_delete_header DELETE_HTTP_HEADER Host will delete the Host header. If Host header occurs more than once all occurrence of the header will be deleted. vii)add rewrite action act_corrupt_header CORRUPT_HTTP_HEADER Host will corrupt the Host header. If Host header occurs more than once all occurrence of the header will be corrupted.

rm rewrite action

Removes a rewrite action.

Synopsis

rm rewrite action <name>

Arguments

name Name of the rewrite action to remove.

Example

rm rewrite action act_before

unset rewrite action

Use this command to remove rewrite action settings.Refer to the set rewrite action command for meanings of the arguments.

Synopsis

unset rewrite action <name>

Rewrite

The entities on which you can perform NetScaler CLI operations:

- rewrite-action
- rewrite-global
- rewrite-param
- rewrite-policy
- rewrite-policylabel

rewrite-global

The following operations can be performed on "rewrite-global":

bind| show| unbind|

bind rewrite global

Activates the specified rewrite policy globally.

Synopsis

bind rewrite global <policyName> <priority>

Arguments

policyName Name of the rewrite policy to activate.

priority Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Must be unique within the label. Policies are evaluated in the order of their priorities, and the first policy that matches the request or response is applied. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.

- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.
- The expression evaluates to a priority number that is smaller than the current policy's priority number.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

type Bind point to which to bind the policy. Available settings function as follows:

- REQ_OVERRIDE - Request override. Binds the policy to the priority request queue.
- REQ_DEFAULT - Binds the policy to the default request queue.
- RES_OVERRIDE - Response override. Binds the policy to the priority response queue. RES_DEFAULT - Binds the policy to the default response queue. OTHERTCP_REQ_OVERRIDE - Binds the policy to the non-HTTP TCP priority request queue. OTHERTCP_REQ_DEFAULT - Binds the policy to the non-HTTP TCP default request queue. OTHERTCP_RES_OVERRIDE - Binds the policy to the non-HTTP TCP priority response queue. OTHERTCP_RES_DEFAULT - Binds the policy to the non-HTTP TCP default response queue. SIPUDP_REQ_OVERRIDE - Binds the policy to the SIP priority request queue. SIPUDP_REQ_DEFAULT - Binds the policy to the SIP default request queue. SIPUDP_RES_OVERRIDE - Binds the policy to the SIP priority response queue. SIPUDP_RES_DEFAULT - Binds the policy to the SIP default response queue.

HTTPQUIC_REQ_OVERRIDE - Binds the policy to the HTTP_QUIC override request queue.
HTTPQUIC_REQ_DEFAULT - Binds the policy to the HTTP_QUIC default request queue.
HTTPQUIC_RES_OVERRIDE - Binds the policy to the HTTP_QUIC override response queue.
HTTPQUIC_RES_DEFAULT - Binds the policy to the HTTP_QUIC default response queue.
MQTT_REQ_OVERRIDE - Binds the policy to the MQTT override request queue.
MQTT_RES_OVERRIDE - Binds the policy to the MQTT override response queue.
MQTT_REQ_DEFAULT - Binds the policy to the MQTT default request queue.
MQTT_RES_DEFAULT - Binds the policy to the MQTT default response queue

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT, OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, OTHERTCP_RES_OVERRIDE, OTHERTCP_RES_DEFAULT, SIPUDP_REQ_OVERRIDE, SIPUDP_REQ_DEFAULT, SIPUDP_RES_OVERRIDE, SIPUDP_RES_DEFAULT, SIPTCP_REQ_OVERRIDE, SIPTCP_REQ_DEFAULT, SIPTCP_RES_OVERRIDE, SIPTCP_RES_DEFAULT, DIAMETER_REQ_OVERRIDE, DIAMETER_REQ_DEFAULT, DIAMETER_RES_OVERRIDE, DIAMETER_RES_DEFAULT, RADIUS_REQ_OVERRIDE, RADIUS_REQ_DEFAULT, RADIUS_RES_OVERRIDE, RADIUS_RES_DEFAULT, DNS_REQ_OVERRIDE, DNS_REQ_DEFAULT, DNS_RES_OVERRIDE, DNS_RES_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, HTTPQUIC_RES_OVERRIDE, HTTPQUIC_RES_DEFAULT, MQTT_REQ_OVERRIDE, MQTT_REQ_DEFAULT, MQTT_RES_OVERRIDE, MQTT_RES_DEFAULT

invoke Terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

labelType Type of invocation. Available settings function as follows:

- reqvserver - Forward the request to the specified request virtual server.
- resvserver - Forward the response to the specified response virtual server.
- policylabel - Invoke the specified policy label.

Possible values: reqvserver, resvserver, policylabel

labelName

- If labelType is policylabel, name of the policy label to invoke.
- If labelType is reqvserver or resvserver, name of the virtual server to which to forward the request of response.

Example

i)bind rewrite global pol9 9 ii)bind rewrite global pol9 9 120 iii)bind rewrite global pol9 9 "HTTP.REQ.HEADER(\\"qh3\\").TYPECAST_NUM_T(DECIMAL)"

show rewrite global

Displays the list of policies bound to the specified rewrite global policy bank. If no policy bank is specified, displays a list of all policies bound to rewrite global.

Synopsis

show rewrite global

Arguments

type The bindpoint to which to policy is bound.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT, OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, OTHERTCP_RES_OVERRIDE, OTHERTCP_RES_DEFAULT, SIPUDP_REQ_OVERRIDE, SIPUDP_REQ_DEFAULT, SIPUDP_RES_OVERRIDE, SIPUDP_RES_DEFAULT, SIPTCP_REQ_OVERRIDE, SIPTCP_REQ_DEFAULT, SIPTCP_RES_OVERRIDE, SIPTCP_RES_DEFAULT, DIAMETER_REQ_OVERRIDE, DIAMETER_REQ_DEFAULT, DIAMETER_RES_OVERRIDE, DIAMETER_RES_DEFAULT, RADIUS_REQ_OVERRIDE, RADIUS_REQ_DEFAULT, RADIUS_RES_OVERRIDE, RADIUS_RES_DEFAULT, DNS_REQ_OVERRIDE, DNS_REQ_DEFAULT, DNS_RES_OVERRIDE, DNS_RES_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, HTTPQUIC_RES_OVERRIDE, HTTPQUIC_RES_DEFAULT, MQTT_REQ_OVERRIDE, MQTT_REQ_DEFAULT, MQTT_RES_OVERRIDE, MQTT_RES_DEFAULT

Output

stateflag policyName Name of the rewrite policy.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke Terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

labelType Type of invocation. Available settings function as follows:

- reqvserver - Forward the request to the specified request virtual server.
- resvserver - Forward the response to the specified response virtual server.
- policylabel - Invoke the specified policy label.

labelName

- If labelType is policylabel, name of the policy label to invoke.
- If labelType is reqvserver or resvserver, name of the virtual server to which to forward the request of response.

numpol The number of policies bound to the bindpoint.

flowType flowtype of the bound rewrite policy.

flags globalBindType devno count

Example

show rewrite global

unbind rewrite global

Unbinds the specified rewrite policy from rewrite global. See the bind rewrite global command for a description of the parameters.

Synopsis

unbind rewrite global <policyName>

Arguments

policyName Name of the rewrite policy to deactivate.

type The bindpoint from which to unbind.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT, OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, OTHERTCP_RES_OVERRIDE, OTHERTCP_RES_DEFAULT, SIPUDP_REQ_OVERRIDE, SIPUDP_REQ_DEFAULT, SIPUDP_RES_OVERRIDE, SIPUDP_RES_DEFAULT, SIPTCP_REQ_OVERRIDE, SIPTCP_REQ_DEFAULT, SIPTCP_RES_OVERRIDE, SIPTCP_RES_DEFAULT, DIAMETER_REQ_OVERRIDE, DIAMETER_REQ_DEFAULT, DIAMETER_RES_OVERRIDE, DIAMETER_RES_DEFAULT, RADIUS_REQ_OVERRIDE, RADIUS_REQ_DEFAULT, RADIUS_RES_OVERRIDE, RADIUS_RES_DEFAULT, DNS_REQ_OVERRIDE,

DNS_REQ_DEFAULT, DNS_RES_OVERRIDE, DNS_RES_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, HTTPQUIC_RES_OVERRIDE, HTTPQUIC_RES_DEFAULT, MQTT_REQ_OVERRIDE, MQTT_REQ_DEFAULT, MQTT_RES_OVERRIDE, MQTT_RES_DEFAULT

priority Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind rewrite global pol9

rewrite-param

The following operations can be performed on "rewrite-param":

unset| show| set|

unset rewrite param

Use this command to remove rewrite param settings.Refer to the set rewrite param command for meanings of the arguments.

Synopsis

unset rewrite param

show rewrite param

Displays the Rewrite parameters.

Synopsis

show rewrite param

Arguments

Output

undefAction Name of the rewrite action.

timeout Execution timeout.

Example

show rewrite param

set rewrite param

Sets the given Rewrite parameter(s).

Synopsis

set rewrite param

Arguments

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an error condition in evaluating the expression. Available settings function as follows:

- NOREWRITE - Do not modify the message.
- RESET - Reset the connection and notify the user's browser, so that the user can resend the request.
- DROP - Drop the message without sending a response to the user. Default value: "NOREWRITE"

timeout Maximum time in milliseconds to allow for processing all the policies and their selected actions without interruption. If the timeout is reached then the evaluation causes an UNDEF to be raised and no further processing is performed. Note that some rewrites may have already been performed. Default value: 3900 Minimum value: 1 Maximum value: 5000

Example

set rewrite param -undefAction RESET -timeout 3000

rewrite-policy

The following operations can be performed on "rewrite-policy":

rm| add| show| stat| rename| unset| set|

rm rewrite policy

Removes the specified rewrite policy.

Synopsis

rm rewrite policy <name>

Arguments

name Name of the rewrite policy to be removed.

Example

rm rewrite policy pol9

add rewrite policy

Creates a rewrite policy, which specifies which requests or responses to rewrite.

Synopsis

add rewrite policy <name> <rule> <action>

Arguments

name Name for the rewrite policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the rewrite policy is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my rewrite policy" or 'my rewrite policy').

rule Expression against which traffic is evaluated.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the rewrite action to perform if the request or response matches this rewrite policy. There are also some built-in actions which can be used. These are:

- NOREWRITE - Send the request from the client to the server or response from the server to the client without making any changes in the message.

- RESET - Resets the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend the request if desired.
- DROP - Drop the request without sending a response to the user.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

comment Any comments to preserve information about this rewrite policy.

logAction Name of messagelog action to use when a request matches this policy.

Example

i)add rewrite policy pol9 "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh3\\")" act_insert ii)add rewrite policy pol9 "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh3\\")" act_insert NOREWRITE iii)add rewrite policy pol9 "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh3\\")" act_insert RESET iii)add rewrite policy pol9 "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh3\\")" act_insert DROP

show rewrite policy

Displays the current settings for the specified rewrite policy. If no policy name is provided, displays a list of all rewrite policies currently configured on the Citrix ADC.

Synopsis

show rewrite policy show rewrite policy stats - alias for 'stat rewrite policy'

Arguments

name Name of the rewrite policy.

Output

stateflag rule Expression against which traffic is evaluated.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.

- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Rewrite action associated with the policy.

undefAction Undef Action associated with the policy.

hits Number of hits.

undefHits Number of Undef hits.

activePolicy Indicates whether policy is bound or not.

boundTo Location where policy is bound

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

description Description of the policy

comment Any comments to preserve information about this rewrite policy.

logAction Name of messagelog action to use when a request matches this policy.

bindPolicyType isDefault A value of true is returned if it is a default rewritepolicy.

vserverType builtin Flag to determine if rewrite policy is built-in or not

feature The feature to be checked while applying this config

type devno count

Example

show rewrite policy

stat rewrite policy

Displays statistics for the specified rewrite policy. If no policy name is specified, displays abbreviated statistics for all rewrite policies currently configured on the Citrix ADC.

Synopsis

stat rewrite policy

Arguments

name Name of the rewrite policy.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Policy undef hits (Undefhits) Number of undef hits on the policy

Example

stat rewrite policy

Related Commands

- stat rewrite policylabel

rename rewrite policy

Renames the specified rewrite policy. You must restart the Citrix ADC to put new name in effect.

Synopsis

rename rewrite policy <name>@ <newName>@

Arguments

name Existing name of the rewrite policy.

newName New name for the rewrite policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my rewrite policy" or 'my rewrite policy').

Example

rename rewrite policy oldname newname

unset rewrite policy

Removes the settings of an existing rewrite policy. Attributes for which a default value is available revert to their default values. See the set rewrite policy command for a description of the parameters..Refer to the set rewrite policy command for meanings of the arguments.

Synopsis

unset rewrite policy <name>

Example

unset rewrite policy pol9 -undefAction

set rewrite policy

Modifies the specified parameters of a rewrite policy.

Synopsis

set rewrite policy <name>

Arguments

name Name of the rewrite policy to modify.

rule Expression against which traffic is evaluated.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the rewrite action to perform if the request or response matches this rewrite policy. There are also some built-in actions which can be used. These are:

- NOREWRITE - Send the request from the client to the server or response from the server to the client without making any changes in the message.
- RESET - Resets the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend the request if desired.
- DROP - Drop the request without sending a response to the user.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

comment Any comments to preserve information about this rewrite policy.

logAction Name of messagelog action to use when a request matches this policy.

Example

set rewrite policy pol9 -rule "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh2\\")"

rewrite-policylabel

The following operations can be performed on "rewrite-policylabel":

rm| bind| show| stat| rename| unbind| add|

rm rewrite policylabel

Removes the specified rewrite policy label.

Synopsis

rm rewrite policylabel <labelName>

Arguments

labelName Name of the rewrite policy label to remove.

Example

rm rewrite policylabel trans_http_url

bind rewrite policylabel

Binds the specified rewrite policy to the specified policy label.

Synopsis

bind rewrite policylabel <labelName> <policyName> <priority>

Arguments

labelName Name of the rewrite policy label to which to bind the policy.

policyName Name of the rewrite policy to bind to the policy label.

priority Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Must be unique within the label. Policies are evaluated in the order of their priorities, and the first policy that matches the request or response is applied. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.

- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.
- The expression evaluates to a priority number that is smaller than the current policy's priority number.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

invoke Suspend evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

labelType Type of invocation. Available settings function as follows:

- reqvserver - Forward the request to the specified request virtual server.
- resvserver - Forward the response to the specified response virtual server.
- policylabel - Invoke the specified policy label.

Possible values: reqvserver, resvserver, policylabel

labelName

- If labelType is policylabel, name of the policy label to invoke.
- If labelType is reqvserver or resvserver, name of the virtual server to which to forward the request or response.

Example

i)bind rewrite policylabel trans_http_url pol_1 1 2 -invoke reqvserver CURRENT ii)bind rewrite policylabel trans_http_url pol_2 2

show rewrite policylabel

Displays the current settings for the specified rewrite policy label. If no policy label is specified, displays a list of all rewrite policy labels currently configured on the Citrix ADC.

Synopsis

show rewrite policylabel

Arguments

labelName Name of the rewrite policy label.

Output

stateflag transform Types of transformations allowed by the policies bound to the label. For Rewrite, the following types are supported:

- http_req - HTTP requests
- http_res - HTTP responses
- othertcp_req - Non-HTTP TCP requests
- othertcp_res - Non-HTTP TCP responses
- url - URLs
- text - Text strings
- clientless_vpn_req - Citrix ADC clientless VPN requests
- clientless_vpn_res - Citrix ADC clientless VPN responses
- sipudp_req - SIP requests
- sipudp_res - SIP responses
- diameter_req - DIAMETER requests
- diameter_res - DIAMETER responses
- radius_req - RADIUS requests
- radius_res - RADIUS responses
- dns_req - DNS requests
- dns_res - DNS responses
- mqtt_req - MQTT requests
- mqtt_res - MQTT responses

numpol Number of polices bound to label.

hits Number of times policy label was invoked.

policyName Name of the rewrite policy to bind to the policy label.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke Suspend evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

labelType Type of invocation. Available settings function as follows:

- reqvserver - Forward the request to the specified request virtual server.
- resvserver - Forward the response to the specified response virtual server.
- policylabel - Invoke the specified policy label.

labelName

- If labelType is policylabel, name of the policy label to invoke.
- If labelType is reqvserver or resvserver, name of the virtual server to which to forward the request or response.

flowType Flowtype of the bound rewrite policy.

description Description of the policylabel

isDefault A value of true is returned if it is a default rewritepolicylabel.

flags comment Any comments to preserve information about this rewrite policy label.

builtin Flag to determine if rewrite policy label is built-in or not

feature The feature to be checked while applying this config

devno count

Example

i)show rewrite policylabel trans_http_url ii)show rewrite policylabel

stat rewrite policylabel

Displays statistics for the specified rewrite policy label. If no policy label name is provided, displays abbreviated statistics for all rewrite policy labels currently configured on the Citrix ADC.

Synopsis

stat rewrite policylabel

Arguments

labelName Name of the rewrite policy label.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy Label Hits (Hits) Number of times policy label was invoked.

rename rewrite policylabel

Renames a rewrite policy label.

Synopsis

rename rewrite policylabel <labelName>@ <newName>@

Arguments

labelName Current name of the policy label.

newName New name for the rewrite policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy label" or 'my policy label').

Example

rename rewrite policylabel oldname newname

unbind rewrite policylabel

Unbinds the specified rewrite policy from the specified policy label. See the bind rewrite policylabel command for a description of the parameters.

Synopsis

unbind rewrite policylabel <labelName> <policyName>

Arguments

labelName Name for the rewrite policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the rewrite policy label is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my rewrite policy label" or 'my rewrite policy label').

policyName Name of the rewrite policy to bind to the policy label.

priority Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind rewrite policylabel trans_http_url pol_1

add rewrite policylabel

Creates a user-defined rewrite policy label.

Synopsis

add rewrite policylabel <labelName> <transform>

Arguments

labelName Name for the rewrite policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the rewrite policy label is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my rewrite policy label" or 'my rewrite policy label').

transform Types of transformations allowed by the policies bound to the label. For Rewrite, the following types are supported:

- http_req - HTTP requests
- http_res - HTTP responses
- othertcp_req - Non-HTTP TCP requests
- othertcp_res - Non-HTTP TCP responses
- url - URLs
- text - Text strings
- clientless_vpn_req - Citrix ADC clientless VPN requests
- clientless_vpn_res - Citrix ADC clientless VPN responses
- sipudp_req - SIP requests
- sipudp_res - SIP responses
- diameter_req - DIAMETER requests
- diameter_res - DIAMETER responses
- radius_req - RADIUS requests
- radius_res - RADIUS responses
- dns_req - DNS requests
- dns_res - DNS responses
- mqtt_req - MQTT requests
- mqtt_res - MQTT responses

Possible values: http_req, http_res, othertcp_req, othertcp_res, url, text, clientless_vpn_req, clientless_vpn_res, sipudp_req, sipudp_res, siptcp_req, siptcp_res, diameter_req, diameter_res, radius_req, radius_res, dns_req, dns_res, httpquic_req, httpquic_res, mqtt_req, mqtt_res

comment Any comments to preserve information about this rewrite policy label.

Example

add rewrite policylabel trans_http_url http_req

router

Router

The entities on which you can perform NetScaler CLI operations:

- router-dynamicRouting
- vtysh

router-dynamicRouting

The following operations can be performed on "router-dynamicRouting":

show| apply| add| unset| set| rm|

show router dynamicRouting

show dynamic routing config from ZebOS daemons

Synopsis

show router dynamicRouting

Arguments

commandString command to be executed

Output

output command output

devno count stateflag

apply router dynamicRouting

apply dynamic routing to ZebOS daemons

Synopsis

apply router dynamicRouting

Arguments

commandString command to be executed

add router dynamicRouting

Add/modify dynamic routing config

Synopsis

add router dynamicRouting

Arguments

commandString command to be executed

unset router dynamicRouting

Unset dynamic routing config.Refer to the set router dynamicRouting command for meanings of the arguments.

Synopsis

unset router dynamicRouting

set router dynamicRouting

Set dynamic routing config

Synopsis

set router dynamicRouting

Arguments

commandString command to be executed

rm router dynamicRouting

Remove dynamic routing config

Synopsis

rm router dynamicRouting

Arguments

commandString command to be executed

vtysh

The following operations can be performed on "vtysh":

vtysh

Enters into the Virtual Teletype Shell (VTYSH) prompt, at which you can configure all the dynamic routing protocols. The Citrix ADC dynamic routing suite is based on ZebOS, the commercial version of GNU Zebra.

Synopsis

vtysh

smpp

Smpp

The entities on which you can perform NetScaler CLI operations:

- smpp-param
- smpp-user

smpp-param

The following operations can be performed on "smpp-param":

show| unset| set|

show smpp param

Displays the SMPP parameters configured on the Citrix ADC.

Synopsis

show smpp param

Arguments

Output

clientmode Mode in which the client binds to the ADC. Applicable settings function as follows:

- TRANSCEIVER - Client can send and receive messages to and from the message center.
- TRANSMITTERONLY - Client can only send messages.
- RECEIVERONLY - Client can only receive messages.

msgQueue Queue SMPP messages if a client that is capable of receiving the destination address messages is not available.

msgQueueSize Maximum number of SMPP messages that can be queued. After the limit is reached, the Citrix ADC sends a deliver_sm_resp PDU, with an appropriate error message, to the message center.

addrton Type of Number, such as an international number or a national number, used in the ESME address sent in the bind request.

addrnpi Numbering Plan Indicator, such as landline, data, or WAP client, used in the ESME address sent in the bind request.

addrrange Set of SME addresses, sent in the bind request, serviced by the ESME.

unset smpp param

Use this command to remove smpp param settings.Refer to the set smpp param command for meanings of the arguments.

Synopsis

unset smpp param

set smpp param

Modifies the SMPP parameters on the Citrix ADC.

Synopsis

set smpp param

Arguments

clientmode Mode in which the client binds to the ADC. Applicable settings function as follows:

- TRANSCEIVER - Client can send and receive messages to and from the message center.
- TRANSMITTERONLY - Client can only send messages.
- RECEIVERONLY - Client can only receive messages.

Possible values: TRANSCEIVER, TRANSMITTERONLY, RECEIVERONLY Default value: TRANSCEIVER

msgQueue Queue SMPP messages if a client that is capable of receiving the destination address messages is not available.

Possible values: ON, OFF Default value: OFF

msgQueueSize Maximum number of SMPP messages that can be queued. After the limit is reached, the Citrix ADC sends a deliver_sm_resp PDU, with an appropriate error message, to the message center. Default value: 10000 Minimum value: 0

addrton Type of Number, such as an international number or a national number, used in the ESME address sent in the bind request. Default value: 0 Minimum value: 0 Maximum value: 256

addrnpi Numbering Plan Indicator, such as landline, data, or WAP client, used in the ESME address sent in the bind request. Default value: 0 Minimum value: 0 Maximum value: 256

addrrange Set of SME addresses, sent in the bind request, serviced by the ESME. Default value: "\\d*"

smpp-user

The following operations can be performed on "smpp-user":

add| rm| show| set|

add smpp user

Adds an SMPP user. The user name and password that you specify in this command are added to the configuration file and used to authenticate the user.

Synopsis

add smpp user <userName> {-password }

Arguments

userName Name of the SMPP user. Must be the same as the user name specified in the SMPP server.

password Password for binding to the SMPP server. Must be the same as the password specified in the SMPP server.

Example

add smpp user johndoe -password secret

rm smpp user

Removes an SMPP user from the Citrix ADC.

Synopsis

rm smpp user <userName>

Arguments

userName Name of the SMPP user to remove.

show smpp user

Displays the specified SMPP user or, if no user is specified, all the SMPP users configured on the appliance.

Synopsis

show smpp user

Arguments

userName Name of the SMPP user.

Output

password Password for binding to the SMPP server. Must be the same as the password specified in the SMPP server.

devno count stateflag

set smpp user

Modifies the password of an existing SMPP user.

Synopsis

set smpp user <userName> {-password }

Arguments

userName Name of the SMPP user.

password The SMPP users password.

Example

set smpp user johndoe supersecret

snmp

snmp-alarm

The following operations can be performed on "snmp-alarm":

show| enable| disable| unset| set|

show snmp alarm

Displays the settings of all SNMP alarms or of the specified SNMP alarm. To display the settings of all the SNMP alarms, run the command without any parameters. To display the settings of a particular SNMP alarm, specify the trapName (Alarm name) of the SNMP alarm.

Synopsis

show snmp alarm

Arguments

trapName Name of the SNMP alarm whose details you want the Citrix ADC to display.

Possible values: CPU-USAGE, AVERAGE-CPU, MEMORY, MGMT-CPU-USAGE, SYNFLOOD, TCP-SYNFLOOD, VSERVER-REQRATE, SERVICE-REQRATE, ENTITY-RXRATE, ENTITY-TXRATE, ENTITY-SYNFLOOD, SERVICE-MAXCLIENTS, HA-STATE-CHANGE, ENTITY-STATE, CONFIG-CHANGE, CONFIG-SAVE, SERVICEGROUP-MEMBER-REQRATE, SERVICEGROUP-MEMBER-MAXCLIENTS, MONITOR-RTO-THRESHOLD, LOGIN-FAILURE, SSL-CERT-EXPIRY, FAN-SPEED-LOW, VOLTAGE-LOW, VOLTAGE-HIGH, TEMPERATURE-HIGH, CPU-TEMPERATURE-HIGH, POWER-SUPPLY-FAILURE, DISK-USAGE-HIGH, INTERFACE-THROUGHPUT-LOW, MON_PROBE_FAILED, HA-VERSION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS, HA-BAD-SECONDARY-STATE, INTERFACE-BW-USAGE, RATE-LIMIT-THRESHOLD-EXCEEDED, ENTITY-NAME-CHANGE, HA-PROP-FAILURE, IP-CONFLICT, PF-RL-RATE-THRESHOLD, PF-RL-PPS-THRESHOLD, PF-RL-RATE-PKTS-DROPPED, PF-RL-PPS-PKTS-DROPPED, APPFW-START-URL, APPFW-DENY-URL, APPFW-VIOLATIONS-TYPE, APPFW-REFERER-HEADER, APPFW-CSRF-TAG, APPFW-COOKIE, APPFW-FIELD-CONSISTENCY, APPFW-BUFFER-OVERFLOW, APPFW-FIELD-FORMAT, APPFW-FILE-UPLOAD-TYPE, APPFW-GRPC, APPFW-GRPC-WEB-JSON, APPFW-GRPC-WEB-TEXT,

APPFW-JSON-DOS, APPFW-JSON-SQL, APPFW-JSON-XSS, APPFW-SAFE-COMMERCE, APPFW-SAFE-OBJECT, APPFW-SESSION-LIMIT, APPFW-SIGNATURE-MATCH, APPFW-POLICY-HIT, APPFW-XSS, APPFW-XML-XSS, APPFW-SQL, APPFW-XML-SQL, APPFW-XML-ATTACHMENT, APPFW-XML-DOS, APPFW-XML-VALIDATION, APPFW-XML-WSI, APPFW-XML-SCHEMA-COMPILE, APPFW-XML-SOAP-FAULT, APPFW-NEW-SIGNATURE-ADDED, APPFW-DEPLOY-RELAXATION-DP, APPFW-LEARNED-RULE-APPLIED-DYN-PROF, APPFW-CMD, APPFW-POSTBODYLIMIT, APPFW-JSON-CMD, APPFW-SQL-GRAM, APPFW-JSON-SQL-GRAM, APPFW-CMD-GRAM, APPFW-JSON-CMD-GRAM, APPFW-BLOCK-KEYWORD, APPFW-JSON-BLOCKKEYWORD, APPFW-BYPASS-LIST, APPFW-DENY-LIST, DNSKEY-EXPIRY, HA-LICENSE-MISMATCH, SSL-CARD-FAILED, SSL-CARD-NORMAL, WARM-RESTART-EVENT, HARD-DISK-DRIVE-ERRORS, COMPACT-FLASH-ERRORS, CALLHOME-UPLOAD-EVENT, 1024KEY-EXCHANGE-RATE, 2048KEY-EXCHANGE-RATE, 4096KEY-EXCHANGE-RATE, SSL-CUR-SESSION-INUSE, CLUSTER-NODE-HEALTH, CLUSTER-NODE-QUORUM, CLUSTER-VERSION-MISMATCH, CLUSTER-CCO-CHANGE, CLUSTER-OVS-CHANGE, CLUSTER-SYNC-FAILURE, CLUSTER-SYNC-PARTIAL-SUCCESS, CLUSTER-PROP-FAILURE, CLUSTER-PROP-EXEC-FAILURE, HA-STICKY-PRIMARY, INBAND-PROTOCOL-VERSION-MISMATCH, SSL-CHIP-REINIT, VRID-STATE-CHANGE, PORT-ALLOC-FAILED, LLDP-REMOTE-CHANGE, DUPLICATE-IPV6, PARTITION-CONFIG-EVENT, PARTITION-SWITCHED, LSN-PORTALLOC-FAILED, LSN-PORTQUOTA-EXCEED, LSN-SESSIONQUOTA-EXCEED, LSN-MEM-RECOVERY-KICKEDIN, VSERVER-SPILLOVER, INCONSISTENT-CONFIGURATION-IN-PPES, PARTITION-RATE-LIMIT, POOLED-LICENSE-ONGRACE, POOLED-LICENSE-PARTIAL, CLUSTER-BACKPLANE-HB-MISSING, GSLB-SITE-MEP-FLAP, DNS-MAXNEGCACHE-USAGE, DNS-MAXCACHE-USAGE, NS-LICENSE-EXPIRY, PKT-RATELIMITING-ATTACK, GSLB-SYNC-STATUS-FLIP, URLFILT-DB-UPDATE-STATUS, URLFILT-INIT-SDK, POOLED-LICENSE-CHECKOUT-FAILURE, MIGRATION-STARTED, MIGRATION-COMPLETE, ECDHE-EXCHANGE-RATE, BOT-SIGNATURE-UPDATE, APPFW-XMLPAYLOAD-CONTENT-TYPE-MISMATCH, PORT-ALLOC-EXCEED, KEK_UPDATE_SUCCESS, KEK_UPDATE_FAILURE, ADC-ANOMALY, SYSLOG-CONNECTION-DROPPED

Output

thresholdValue The high threshold value.

normalValue The normal threshold value.

time The time interval for the SYNFLOOD alarm.

state Current state of the SNMP alarm. The Citrix ADC generates trap messages only for SNMP alarms that are enabled. Some alarms are enabled by default, but you can disable them.

severity The severity of this alarm.

logging The log status of the alarm.

flags timeout If DB is enabled and clear config is fired, then to reset timeinterval of alarm, corresponding default time value is needed. This hidden argument holds the default time value for the corresponding alarm.

devno count stateflag

enable snmp alarm

Enables or disables an SNMP alarm. The Citrix ADC looks for conditions specified in the enabled SNMP alarms. When the condition in any enabled SNMP alarm is met, the appliance generates an SNMP trap message. It does not look for conditions specified in disabled SNMP alarms and therefore does not generate an SNMP trap message when the condition in any disabled SNMP alarm is met. Some alarms are enabled by default, but you can disable them.

Synopsis

enable snmp alarm <trapName> ...

Arguments

trapName Name of the SNMP alarm. This parameter is required for identifying the SNMP alarm.

Possible values: CPU-USAGE, AVERAGE-CPU, MEMORY, MGMT-CPU-USAGE, SYNFLOOD, TCP-SYNFLOOD, VSERVER-REQRATE, SERVICE-REQRATE, ENTITY-RXRATE, ENTITY-TXRATE, ENTITY-SYNFLOOD, SERVICE-MAXCLIENTS, HA-STATE-CHANGE, ENTITY-STATE, CONFIG-CHANGE, CONFIG-SAVE, SERVICEGROUP-MEMBER-REQRATE, SERVICEGROUP-MEMBER-MAXCLIENTS, MONITOR-RTO-THRESHOLD, LOGIN-FAILURE, SSL-CERT-EXPIRY, FAN-SPEED-LOW, VOLTAGE-LOW, VOLTAGE-HIGH, TEMPERATURE-HIGH, CPU-TEMPERATURE-HIGH, POWER-SUPPLY-FAILURE, DISK-USAGE-HIGH, INTERFACE-THROUGHPUT-LOW, MON_PROBE_FAILED, HA-VERSION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS, HA-BAD-SECONDARY-STATE, INTERFACE-BW-USAGE, RATE-LIMIT-THRESHOLD-EXCEEDED, ENTITY-NAME-CHANGE, HA-PROP-FAILURE, IP-CONFLICT, PF-RL-RATE-THRESHOLD, PF-RL-PPS-THRESHOLD, PF-RL-RATE-PKTS-DROPPED, PF-RL-PPS-PKTS-DROPPED, APPFW-START-URL, APPFW-DENY-URL, APPFW-VIOLATIONS-TYPE, APPFW-REFERER-HEADER, APPFW-CSRF-TAG, APPFW-COOKIE, APPFW-FIELD-CONSISTENCY, APPFW-BUFFER-OVERFLOW, APPFW-FIELD-FORMAT, APPFW-FILE-UPLOAD-TYPE, APPFW-GRPC, APPFW-GRPC-WEB-JSON, APPFW-GRPC-WEB-TEXT, APPFW-JSON-DOS, APPFW-JSON-SQL, APPFW-JSON-XSS, APPFW-SAFE-COMMERCE,

APPFW-SAFE-OBJECT, APPFW-SESSION-LIMIT, APPFW-SIGNATURE-MATCH, APPFW-POLICY-HIT, APPFW-XSS, APPFW-XML-XSS, APPFW-SQL, APPFW-XML-SQL, APPFW-XML-ATTACHMENT, APPFW-XML-DOS, APPFW-XML-VALIDATION, APPFW-XML-WSI, APPFW-XML-SCHEMA-COMPILE, APPFW-XML-SOAP-FAULT, APPFW-NEW-SIGNATURE-ADDED, APPFW-DEPLOY-RELAXATION-DP, APPFW-LEARNED-RULE-APPLIED-DYN-PROF, APPFW-CMD, APPFW-POSTBODYLIMIT, APPFW-JSON-CMD, APPFW-SQL-GRAM, APPFW-JSON-SQL-GRAM, APPFW-CMD-GRAM, APPFW-JSON-CMD-GRAM, APPFW-BLOCK-KEYWORD, APPFW-JSON-BLOCKKEYWORD, APPFW-BYPASS-LIST, APPFW-DENY-LIST, DNSKEY-EXPIRY, HA-LICENSE-MISMATCH, SSL-CARD-FAILED, SSL-CARD-NORMAL, WARM-RESTART-EVENT, HARD-DISK-DRIVE-ERRORS, COMPACT-FLASH-ERRORS, CALLHOME-UPLOAD-EVENT, 1024KEY-EXCHANGE-RATE, 2048KEY-EXCHANGE-RATE, 4096KEY-EXCHANGE-RATE, SSL-CUR-SESSION-INUSE, CLUSTER-NODE-HEALTH, CLUSTER-NODE-QUORUM, CLUSTER-VERSION-MISMATCH, CLUSTER-CCO-CHANGE, CLUSTER-OVS-CHANGE, CLUSTER-SYNC-FAILURE, CLUSTER-SYNC-PARTIAL-SUCCESS, CLUSTER-PROP-FAILURE, CLUSTER-PROP-EXEC-FAILURE, HA-STICKY-PRIMARY, INBAND-PROTOCOL-VERSION-MISMATCH, SSL-CHIP-REINIT, VRID-STATE-CHANGE, PORT-ALLOC-FAILED, LLDP-REMOTE-CHANGE, DUPLICATE-IPV6, PARTITION-CONFIG-EVENT, PARTITION-SWITCHED, LSN-PORTALLOC-FAILED, LSN-PORTQUOTA-EXCEED, LSN-SESSIONQUOTA-EXCEED, LSN-MEM-RECOVERY-KICKEDIN, VSERVER-SPILLOVER, INCONSISTENT-CONFIGURATION-IN-PPES, PARTITION-RATE-LIMIT, POOLED-LICENSE-ONGRACE, POOLED-LICENSE-PARTIAL, CLUSTER-BACKPLANE-HB-MISSING, GSLB-SITE-MEP-FLAP, DNS-MAXNEGCACHE-USAGE, DNS-MAXCACHE-USAGE, NS-LICENSE-EXPIRY, PKT-RATELIMITING-ATTACK, GSLB-SYNC-STATUS-FLIP, URLFILT-DB-UPDATE-STATUS, URLFILT-INIT-SDK, POOLED-LICENSE-CHECKOUT-FAILURE, MIGRATION-STARTED, MIGRATION-COMPLETE, ECDHE-EXCHANGE-RATE, BOT-SIGNATURE-UPDATE, APPFW-XMLPAYLOAD-CONTENT-TYPE-MISMATCH, PORT-ALLOC-EXCEED, KEK_UPDATE_SUCCESS, KEK_UPDATE_FAILURE, ADC-ANOMALY, SYSLOG-CONNECTION-DROPPED

Example

enable snmp alarm VSERVER-REQRATE enable snmp alarm CPU SYNFLOOD

disable snmp alarm

Disables an SNMP alarm. The Citrix ADC does not generate trap messages for SNMP alarms that are disabled. Some alarms are enabled by default, but you can disable them.

Synopsis

disable snmp alarm <trapName> ...

Arguments

trapName Name of the SNMP alarm. This parameter is required for identifying the SNMP alarm.

Possible values: CPU-USAGE, AVERAGE-CPU, MEMORY, MGMT-CPU-USAGE, SYNFLOOD, TCP-SYNFLOOD, VSERVER-REQRATE, SERVICE-REQRATE, ENTITY-RXRATE, ENTITY-TXRATE, ENTITY-SYNFLOOD, SERVICE-MAXCLIENTS, HA-STATE-CHANGE, ENTITY-STATE, CONFIG-CHANGE, CONFIG-SAVE, SERVICEGROUP-MEMBER-REQRATE, SERVICEGROUP-MEMBER-MAXCLIENTS, MONITOR-RTO-THRESHOLD, LOGIN-FAILURE, SSL-CERT-EXPIRY, FAN-SPEED-LOW, VOLTAGE-LOW, VOLTAGE-HIGH, TEMPERATURE-HIGH, CPU-TEMPERATURE-HIGH, POWER-SUPPLY-FAILURE, DISK-USAGE-HIGH, INTERFACE-THROUGHPUT-LOW, MON_PROBE_FAILED, HA-VERSION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS, HA-BAD-SECONDARY-STATE, INTERFACE-BW-USAGE, RATE-LIMIT-THRESHOLD-EXCEEDED, ENTITY-NAME-CHANGE, HA-PROP-FAILURE, IP-CONFLICT, PF-RL-RATE-THRESHOLD, PF-RL-PPS-THRESHOLD, PF-RL-RATE-PKTS-DROPPED, PF-RL-PPS-PKTS-DROPPED, APPFW-START-URL, APPFW-DENY-URL, APPFW-VIOLATIONS-TYPE, APPFW-REFERER-HEADER, APPFW-CSRF-TAG, APPFW-COOKIE, APPFW-FIELD-CONSISTENCY, APPFW-BUFFER-OVERFLOW, APPFW-FIELD-FORMAT, APPFW-FILE-UPLOAD-TYPE, APPFW-GRPC, APPFW-GRPC-WEB-JSON, APPFW-GRPC-WEB-TEXT, APPFW-JSON-DOS, APPFW-JSON-SQL, APPFW-JSON-XSS, APPFW-SAFE-COMMERCE, APPFW-SAFE-OBJECT, APPFW-SESSION-LIMIT, APPFW-SIGNATURE-MATCH, APPFW-POLICY-HIT, APPFW-XSS, APPFW-XML-XSS, APPFW-SQL, APPFW-XML-SQL, APPFW-XML-ATTACHMENT, APPFW-XML-DOS, APPFW-XML-VALIDATION, APPFW-XML-WSI, APPFW-XML-SCHEMA-COMPILE, APPFW-XML-SOAP-FAULT, APPFW-NEW-SIGNATURE-ADDED, APPFW-DEPLOY-RELAXATION-DP, APPFW-LEARNED-RULE-APPLIED-DYN-PROF, APPFW-CMD, APPFW-POSTBODYLIMIT, APPFW-JSON-CMD, APPFW-SQL-GRAM, APPFW-JSON-SQL-GRAM, APPFW-CMD-GRAM, APPFW-JSON-CMD-GRAM, APPFW-BLOCK-KEYWORD, APPFW-JSON-BLOCKKEYWORD, APPFW-BYPASS-LIST, APPFW-DENY-LIST, DNSKEY-EXPIRY, HA-LICENSE-MISMATCH, SSL-CARD-FAILED, SSL-CARD-NORMAL, WARM-RESTART-EVENT, HARD-DISK-DRIVE-ERRORS, COMPACT-FLASH-ERRORS, CALLHOME-UPLOAD-EVENT, 1024KEY-EXCHANGE-RATE, 2048KEY-EXCHANGE-RATE, 4096KEY-EXCHANGE-RATE, SSL-CUR-SESSION-INUSE, CLUSTER-NODE-HEALTH, CLUSTER-NODE-QUORUM, CLUSTER-VERSION-MISMATCH, CLUSTER-CCO-CHANGE, CLUSTER-OVS-CHANGE, CLUSTER-SYNC-FAILURE, CLUSTER-SYNC-PARTIAL-SUCCESS, CLUSTER-PROP-FAILURE, CLUSTER-PROP-EXEC-FAILURE, HA-STICKY-PRIMARY, INBAND-PROTOCOL-VERSION-MISMATCH, SSL-CHIP-REINIT, VRID-STATE-CHANGE, PORT-ALLOC-FAILED, LLDP-REMOTE-CHANGE, DUPLICATE-IPV6, PARTITION-CONFIG-EVENT, PARTITION-SWITCHED, LSN-PORTALLOC-FAILED, LSN-PORTQUOTA-EXCEED, LSN-SESSIONQUOTA-EXCEED, LSN-MEM-RECOVERY-

KICKEDIN, VSERVER-SPILLOVER, INCONSISTENT-CONFIGURATION-IN-PPES, PARTITION-RATE-LIMIT, POOLED-LICENSE-ONGRACE, POOLED-LICENSE-PARTIAL, CLUSTER-BACKPLANE-HB-MISSING, GSLB-SITE-MEP-FLAP, DNS-MAXNEGCACHE-USAGE, DNS-MAXCACHE-USAGE, NS-LICENSE-EXPIRY, PKT-RATELIMITING-ATTACK, GSLB-SYNC-STATUS-FLIP, URLFILT-DB-UPDATE-STATUS, URLFILT-INIT-SDK, POOLED-LICENSE-CHECKOUT-FAILURE, MIGRATION-STARTED, MIGRATION-COMPLETE, ECDHE-EXCHANGE-RATE, BOT-SIGNATURE-UPDATE, APPFW-XMLPAYLOAD-CONTENT-TYPE-MISMATCH, PORT-ALLOC-EXCEED, KEK_UPDATE_SUCCESS, KEK_UPDATE_FAILURE, ADC-ANOMALY, SYSLOG-CONNECTION-DROPPED

Example

disable snmp alarm VSERVER-REQRATE disable snmp alarm CPU SYNFLOOD

unset snmp alarm

Resets the specified parameters of an SNMP alarm to their default settings..Refer to the set snmp alarm command for meanings of the arguments.

Synopsis

unset snmp alarm <trapName>

Example

unset snmp alarm VSERVER-REQRATE

set snmp alarm

Configures an SNMP alarm. You must enable and configure alarms to generate enterprise-specific trap messages. The Citrix ADC sends these trap messages only to trap listeners of type (class) SPECIFIC. The SNMP alarms are either event based or threshold based.

The Citrix ADC supports the following user configurable alarms: HA-STATE-CHANGE: Change to primary/secondary CPU-USAGE: Individual CPU usage AVERAGE-CPU: Average CPU usage MGMT-CPU: Management CPU usage ENTITY-STATE: Entity state change SYNFLOOD: Global unacknowledged SYN count MEMORY: Memory usage VSERVER-REQRATE: Vserver specific request rate SERVICE-REQRATE: Service specific request rate ENTITY-RXRATE: Entity specific Rx bytes per sec ENTITY-TXRATE: Entity specific Tx bytes per sec ENTITY-SYNFLOOD: Entity specific unacknowledged SYN count CONFIG-CHANGE: System configuration changed SERVICE-MAXCLIENTS: Service hit max-client limit CONFIG-SAVE: System configuration was saved SERVICEGROUP-MEMBER-REQRATE: Request rate on a service group member

SERVICEGROUP-MEMBER-MAXCLIENTS: Service group member hits max-client MONITOR-RTO-THRESHOLD: Monitor probe response timeout LOGIN-FAILURE: GUI/CLI/API login failure SSL-CERT-EXPIRY: Certificate expiry FAN-SPEED-LOW: Low fan speed VOLTAGE-LOW: Low voltage VOLTAGE-HIGH: High Voltage TEMPERATURE-HIGH: High temperature CPU-TEMPERATURE-HIGH: High CPU temperature POWER-SUPPLY-FAILURE: Power supply failure DISK-USAGE-HIGH: High disk usage INTERFACE-THROUGHPUT-LOW: Low Interface throughput MON_PROBE_FAILED: Monitor probe failure HA-VERSION-MISMATCH: HA Citrix ADC's OS version mismatch HA-SYNC-FAILURE: HA config synchronization failure HA-NO-HEARTBEATS: No HA hearbeats HA-BAD-SECONDARY-STATE: Secondary state DOWN/ UNKNOWN/STAY SECONDARY INTERFACE-BW-USAGE: System aggregate BW usage RATE-LIMIT-THRESHOLD-EXCEEDED: Client exceed rate-limit threshold ENTITY-NAME-CHANGE: Entity name change HA-PROP-FAILURE: HA config propagation failure IP-CONFLICT: IP conflict PF-RL-RATE-THRESHOLD: Platform rate limit in Mbps PF-RL-PPS-THRESHOLD: Platform packets per second limit PF-RL-RATE-PKTS-DROPPED: Packet Drops due to platform rate limit PF-RL-PPS-PKTS-DROPPED: Packet Drops due to platform packet per sec limit APPFW-START-URL: AppFirewall Start URL violation APPFW-DENY-URL: AppFirewall Deny URL violation APPFW-REFERER-HEADER: AppFirewall Referer Header violation APPFW-CSRF-TAG: AppFirewall CSRF Tag violation APPFW-COOKIE: AppFirewall Cookie violation APPFW-FIELD-CONSISTENCY: AppFirewall Field Consistency violation APPFW-BUFFER-OVERFLOW: AppFirewall Buffer Overflow violation APPFW-POSTBODYLIMIT: AppFirewall Post Body Limit violation APPFW-FIELD-FORMAT: AppFirewall Field Format violation APPFW-JSON-DOS: AppFirewall JSON DoS violation APPFW-JSON-SQL: AppFirewall JSON SQL violation APPFW-JSON-SQL-GRAM: AppFirewall JSON SQL violation (detected by SQL Grammar) APPFW-BLOCK-KEYWORD: AppFirewall Block Keyword violation APPFW-JSON-BLOCKKEYWORD: AppFirewall JSON Block Keyword violation APPFW-BYPASS-LIST: AppFirewall Bypass List Rule Hit APPFW-DENY-LIST: AppFirewall Deny List Rule Hit APPFW-JSON-XSS: AppFirewall JSON Cross Site Scripting violation APPFW-SAFE-COMMERCE: AppFirewall Safe Commerce violation APPFW-SAFE-OBJECT: AppFirewall Safe Object violation APPFW-POLICY-HIT: AppFirewall Policy Hit APPFW-VIOLATIONS-TYPE: AppFirewall Content Type violation APPFW-XSS: AppFirewall Cross Site Scripting violation APPFW-SIGNATURE-MATCH: AppFirewall Signature violation APPFW-XML-XSS: AppFirewall XML Cross Site Scripting violation APPFW-SQL: AppFirewall SQL violation APPFW-XML-SQL: AppFirewall XML SQL violation APPFW-SQL-GRAM: AppFirewall SQL violation reported by SQL Grammar APPFW-CMD: AppFirewall CMD Injection violation APPFW-CMD-GRAM: AppFirewall CMD violation reported by SQL Grammar APPFW-JSON-CMD: AppFirewall JSON CMD Injection violation APPFW-JSON-CMD-GRAM: AppFirewall JSON CMD violation (detected by CMD Grammar) APPFW-XML-ATTACHMENT: AppFirewall XML Attachment violation APPFW-XML-DOS: AppFirewall XML DoS violation APPFW-XML-

VALIDATION: AppFirewall XML Validation violation APPFW-XML-WSI: AppFirewall XML WSI violation APPFW-XML-SCHEMA-COMPILE: AppFirewall XML Schema Compile violation APPFW-XML-SOAP-FAULT: AppFirewall XML Soap Fault violation DNSKEY-EXPIRY: DNSKEY expiry HA-LICENSE-MISMATCH: HA Citrix ADC's license mismatch APPFW-SESSION-LIMIT: AppFirewall Session Limit reached SSL-CARD-FAILED: SSL Card Failed SSL-CARD-NORMAL: SSL Card Normal WARM-RESTART-EVENT: Warm Restart Event Occurred HARD-DISK-DRIVE-ERRORS: Hard Disk Drive Errors COMPACT-FLASH-ERRORS: Compact Flash Errors CALLHOME-UPLOAD-EVENT: Attempt to upload Show Tech Support Archive 1024KEY-EXCHANGE-RATE: 1024 Key Exchange Rate 2048KEY-EXCHANGE-RATE: 2048 Key Exchange Rate 4096KEY-EXCHANGE-RATE: 4096 Key Exchange Rate SSL-CUR-SESSION-INUSE: SSL Current Sessions In Use SYSLOG-CONNECTION-DROPPED: Syslog server connection dropped CLUSTER-NODE-HEALTH: Cluster Node Health State Change CLUSTER-NODE-QUORUM: Cluster Node View has Quorum CLUSTER-VERSION-MISMATCH: Cluster Node Version Mismatch CLUSTER-CCO-CHANGE: Cluster Configuration Coordinator Change CLUSTER-OVS-CHANGE: Cluster Operational View Set Change CLUSTER-SYNC-FAILURE: Cluster Config Synchronization Failure CLUSTER-SYNC-PARTIAL-SUCCESS: Cluster Config Synchronization Partial Success CLUSTER-PROP-FAILURE: Cluster Config Propagation Failure CLUSTER-PROP-EXEC-FAILURE: Cluster propagated command Failure HA-STICKY-PRIMARY: Fixed primary state owing to max HA flips INBAND-PROTOCOL-VERSION-MISMATCH: Inband protocol mismatch between BR and QoSd SSL-CHIP-REINIT: SSL Chip Reinit VRID-STATE-CHANGE: VRID State Change PORT-ALLOC-FAILED: Port Alloc Failed LLDP-REMOTE-CHANGE: LLDP Remote Change DUPLICATE-IPV6: IPv6 Address got duplicated PARTITION-CONFIG-EVENT: Partition Added/ removed PARTITION-SWITCHED: Partition Swicthed LSN-PORTALLOC-FAILED: LSN Port Allocation Failed LSN-PORTQUOTA-EXCEED: LSN Port Quota Exceeded LSN-SESSIONQUOTA-EXCEED: LSN Session Quota Exceeded LSN-MEM-RECOVERY-KICKEDIN: LSN Memory Recovery Kicked-in VSERVER-SPILLOVER: Vserver spillover occurred PARTITION-RATE-LIMIT: Partition bandwidth, connection and memory limit/threshold exceeded POOLED-LICENSE-ONGRACE: Pooled license running on grace POOLED-LICENSE-PARTIAL: Pooled license partial capacity CLUSTER-BACKPLANE-HB-MISSING: Heartbeats are missing on backplane GSLB-SITE-MEP-FLAP: GSLB site MEP flap DNS-MAXNEGCACHE-USAGE: Max negative cache usage limit for DNS DNS-MAXCACHE-USAGE: Max cache usage limit for DNS TCP-SYNFLOOD: SYN Flood for TCP NS-LICENSE-EXPIRY: Citrix ADC license expiry PKT-RATELIMITING-ATTACK: Detected packet ratelimiting attack GSLB-SYNC-STATUS-FLIP: GSLB sync status flip URLFILT-DB-UPDATE-STATUS: Urlfiltering Database Update Status URLFILT-INIT-SDK: Urlfiltering SDK Initialization APPFW-NEW-SIGNATURE-ADDED: New Appfw Signature Imported POOLED-LICENSE-CHECKOUT-FAILURE: Pooled license checkout failure APPFW-FILE-UPLOAD-TYPE: Appfw File Upload Type Violation MIGRATION-STARTED: Migration has been initiated

MIGRATION-COMPLETE: Migration is complete on N1 APPFW-DEPLOY-RELAXATION-DP: Appfw Relaxation ready to be deployed APPFW-LEARNED-RULE-APPLIED-DYN-PROF: Appfw learned rule applied ECDHE-EXCHANGE-RATE: ecdhe based transactions per second BOT-SIGNATURE-UPDATE: Bot Signature Auto Update APPFW-XMLPAYLOAD-CONTENT-TYPE-MISMATCH: Appfw XML Payload Content-Type Mismatch Violation INCONSISTENT-CONFIGURATION-IN-PPES: Inconsistent configuration across multiple PPEs APPFW-GRPC: gRPC request blocked by appfw APPFW-GRPC-WEB-TEXT: gRPC-web text request blocked by appfw APPFW-GRPC-WEB-JSON: gRPC-web JSON request blocked by appfw PORT-ALLOC-EXCEED: Port allocation percentage exceeds the configured value KEK_UPDATE_SUCCESS: Update KEK successful KEK_UPDATE_FAILURE: Update KEK failure ADC-ANOMALY: ADC Anomaly detected

For the purposes of this command, entity includes vservers and services.

Synopsis

set snmp alarm <trapName> [-thresholdValue <positive_integer>]

Arguments

trapName Name of the SNMP alarm. This parameter is required for identifying the SNMP alarm and cannot be modified.

Possible values: CPU-USAGE, AVERAGE-CPU, MEMORY, MGMT-CPU-USAGE, SYNFLOOD, TCP-SYNFLOOD, VSERVER-REQRATE, SERVICE-REQRATE, ENTITY-RXRATE, ENTITY-TXRATE, ENTITY-SYNFLOOD, SERVICE-MAXCLIENTS, HA-STATE-CHANGE, ENTITY-STATE, CONFIG-CHANGE, CONFIG-SAVE, SERVICEGROUP-MEMBER-REQRATE, SERVICEGROUP-MEMBER-MAXCLIENTS, MONITOR-RTO-THRESHOLD, LOGIN-FAILURE, SSL-CERT-EXPIRY, FAN-SPEED-LOW, VOLTAGE-LOW, VOLTAGE-HIGH, TEMPERATURE-HIGH, CPU-TEMPERATURE-HIGH, POWER-SUPPLY-FAILURE, DISK-USAGE-HIGH, INTERFACE-THROUGHPUT-LOW, MON_PROBE_FAILED, HA-VERSION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS, HA-BAD-SECONDARY-STATE, INTERFACE-BW-USAGE, RATE-LIMIT-THRESHOLD-EXCEEDED, ENTITY-NAME-CHANGE, HA-PROP-FAILURE, IP-CONFLICT, PF-RL-RATE-THRESHOLD, PF-RL-PPS-THRESHOLD, PF-RL-RATE-PKTS-DROPPED, PF-RL-PPS-PKTS-DROPPED, APPFW-START-URL, APPFW-DENY-URL, APPFW-VIOLATIONS-TYPE, APPFW-REFERER-HEADER, APPFW-CSRF-TAG, APPFW-COOKIE, APPFW-FIELD-CONSISTENCY, APPFW-BUFFER-OVERFLOW, APPFW-FIELD-FORMAT, APPFW-FILE-UPLOAD-TYPE, APPFW-GRPC, APPFW-GRPC-WEB-JSON, APPFW-GRPC-WEB-TEXT, APPFW-JSON-DOS, APPFW-JSON-SQL, APPFW-JSON-XSS, APPFW-SAFE-COMMERCE, APPFW-SAFE-OBJECT, APPFW-SESSION-LIMIT, APPFW-SIGNATURE-MATCH, APPFW-

POLICY-HIT, APPFW-XSS, APPFW-XML-XSS, APPFW-SQL, APPFW-XML-SQL, APPFW-XML-ATTACHMENT, APPFW-XML-DOS, APPFW-XML-VALIDATION, APPFW-XML-WSI, APPFW-XML-SCHEMA-COMPILE, APPFW-XML-SOAP-FAULT, APPFW-NEW-SIGNATURE-ADDED, APPFW-DEPLOY-RELAXATION-DP, APPFW-LEARNED-RULE-APPLIED-DYN-PROF, APPFW-CMD, APPFW-POSTBODYLIMIT, APPFW-JSON-CMD, APPFW-SQL-GRAM, APPFW-JSON-SQL-GRAM, APPFW-CMD-GRAM, APPFW-JSON-CMD-GRAM, APPFW-BLOCK-KEYWORD, APPFW-JSON-BLOCKKEYWORD, APPFW-BYPASS-LIST, APPFW-DENY-LIST, DNSKEY-EXPIRY, HA-LICENSE-MISMATCH, SSL-CARD-FAILED, SSL-CARD-NORMAL, WARM-RESTART-EVENT, HARD-DISK-DRIVE-ERRORS, COMPACT-FLASH-ERRORS, CALLHOME-UPLOAD-EVENT, 1024KEY-EXCHANGE-RATE, 2048KEY-EXCHANGE-RATE, 4096KEY-EXCHANGE-RATE, SSL-CUR-SESSION-INUSE, CLUSTER-NODE-HEALTH, CLUSTER-NODE-QUORUM, CLUSTER-VERSION-MISMATCH, CLUSTER-CCO-CHANGE, CLUSTER-OVS-CHANGE, CLUSTER-SYNC-FAILURE, CLUSTER-SYNC-PARTIAL-SUCCESS, CLUSTER-PROP-FAILURE, CLUSTER-PROP-EXEC-FAILURE, HA-STICKY-PRIMARY, INBAND-PROTOCOL-VERSION-MISMATCH, SSL-CHIP-REINIT, VRID-STATE-CHANGE, PORT-ALLOC-FAILED, LLDP-REMOTE-CHANGE, DUPLICATE-IPV6, PARTITION-CONFIG-EVENT, PARTITION-SWITCHED, LSN-PORTALLOC-FAILED, LSN-PORTQUOTA-EXCEED, LSN-SESSIONQUOTA-EXCEED, LSN-MEM-RECOVERY-KICKEDIN, VSERVER-SPILLOVER, INCONSISTENT-CONFIGURATION-IN-PPES, PARTITION-RATE-LIMIT, POOLED-LICENSE-ONGRACE, POOLED-LICENSE-PARTIAL, CLUSTER-BACKPLANE-HB-MISSING, GSLB-SITE-MEP-FLAP, DNS-MAXNEGCACHE-USAGE, DNS-MAXCACHE-USAGE, NS-LICENSE-EXPIRY, PKT-RATELIMITING-ATTACK, GSLB-SYNC-STATUS-FLIP, URLFILT-DB-UPDATE-STATUS, URLFILT-INIT-SDK, POOLED-LICENSE-CHECKOUT-FAILURE, MIGRATION-STARTED, MIGRATION-COMPLETE, ECDHE-EXCHANGE-RATE, BOT-SIGNATURE-UPDATE, APPFW-XMLPAYLOAD-CONTENT-TYPE-MISMATCH, PORT-ALLOC-EXCEED, KEK_UPDATE_SUCCESS, KEK_UPDATE_FAILURE, ADC-ANOMALY, SYSLOG-CONNECTION-DROPPED

thresholdValue Value for the high threshold. The Citrix ADC generates an SNMP trap message when the value of the attribute associated with the alarm is greater than or equal to the specified high threshold value. Minimum value: 1

normalValue Value for the normal threshold. A trap message is generated if the value of the respective attribute falls to or below this value after exceeding the high threshold. Minimum value: 1

time Interval, in seconds, at which the Citrix ADC generates SNMP trap messages when the conditions specified in the SNMP alarm are met.Can be specified for the following alarms: SYNFLOOD, HA-VERSION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS,HA-BAD-SECONDARY-STATE, CLUSTER-NODE-HEALTH, CLUSTER-NODE-QUORUM, CLUSTER-

VERSION-MISMATCH, CLUSTER-BKHB-FAILED, PORT-ALLOC-FAILED, COMPACT-FLASH-ERRORS, HARD-DISK-DRIVE-ERRORS and APPFW traps. Default trap time intervals: SYNFLOOD and APPFW traps = 1sec, PORT-ALLOC-FAILED = 3600sec(1 hour), PORT-ALLOC-EXCEED = 3600sec(1 hour), Other Traps = 86400sec(1 day) Default value: 1

state Current state of the SNMP alarm. The Citrix ADC generates trap messages only for SNMP alarms that are enabled. Some alarms are enabled by default, but you can disable them.

Possible values: ENABLED, DISABLED Default value: ENABLED

severity Severity level assigned to trap messages generated by this alarm. The severity levels are, in increasing order of severity, Informational, Warning, Minor, Major, and Critical. This parameter is useful when you want the Citrix ADC to send trap messages to a trap listener on the basis of severity level. Trap messages with a severity level lower than the specified level (in the trap listener entry) are not sent.

Possible values: Critical, Major, Minor, Warning, Informational Default value: Unknown

logging Logging status of the alarm. When logging is enabled, the Citrix ADC logs every trap message that is generated for this alarm.

Possible values: ENABLED, DISABLED Default value: ENABLED

Example

set snmp alarm VSERVER-REQRATE -thresholdValue 10000 -normalValue 100

Related Commands

- add snmp trap

Snmp

The entities on which you can perform NetScaler CLI operations:

- snmp-alarm
- snmp-community
- snmp-engineId
- snmp-group
- snmp-manager
- snmp-mib

- snmp-oid
- snmp-option
- snmp
- snmp-stats
- snmp-trap
- snmp-user
- snmp-view

snmp-community

The following operations can be performed on "snmp-community":

rm| add| show|

rm snmp community

Removes an SNMP community from the Citrix ADC. After you remove the SNMP community, the appliance does not respond to any SNMP queries that contain that community string.

Synopsis

rm snmp community <communityName>

Arguments

communityName The name of the SNMP community.

Example

rm snmp community public

add snmp community

Creates an SNMP community, which is a password (string) used to authenticate SNMP queries from SNMP managers. You can associate it with any of the following SNMP query types: GET, GET NEXT, ALL, GET BULK. You can associate one or more community strings with each query type. For example, if you associate two community strings, such as Example and Test, with the query type GET NEXT, the Citrix ADC considers only those GET NEXT SNMP query packets that contain Example or Test as the community string.

Synopsis

add snmp community <communityName> <permissions>

Arguments

communityName The SNMP community string. Can consist of 1 to 31 characters that include uppercase and lowercase letters,numbers and special characters.

The following requirement applies only to the Citrix ADC CLI: If the string includes one or more spaces, enclose the name in double or single quotation marks (for example, "my string" or 'my string').

permissions The SNMP V1 or V2 query-type privilege that you want to associate with this SNMP community.

Possible values: GET, GET_NEXT, GET_BULK, SET, ALL

Example

add snmp community public ALL add snmp community a#12ab GET_BULK

show snmp community

Displays the SNMP v1 or v2 query-type privileges (such as GET, GET NEXT, ALL, or GET BULK) that have been set for all SNMP communities or for the specified SNMP community. To display the settings of all the SNMP communities, run the command without any parameters. To display the settings of a particular SNMP community, specify the name of the SNMP community.

Synopsis

show snmp community

Arguments

communityName The name of the SNMP community whose SNMP v1 or v2 query type privilege setting, such as GET, GET NEXT, ALL, or GET BULK, you want the Citrix ADC to display.

Output

permissions The SNMP V1 or V2 query-type privilege that you want to associate with this SNMP community.

devno count stateflag

Example

show snmp community

snmp-engineId

The following operations can be performed on "snmp-engineId":

set| show| unset|

set snmp engineId

Modifies the SNMPv3 engine identification (ID) on the Citrix ADC. Caution: Changing the ID of the SNMPv3 engine invalidates the current SNMP users. You have to reconfigure the SNMP users in the SNMP managers. The SNMPv3 engine has an identification (ID) that uniquely identifies it on the appliance and is used in the communication between the SNMPv3 user and the SNMPv3 engine. The engine ID is preconfigured by Citrix and is based on the MAC address of one of its interfaces. Overriding the engine ID is not necessary, but you can change it.

Synopsis

set snmp engineId <engineID>

Arguments

engineID A hexadecimal value of at least 10 characters, uniquely identifying the engineid

ownerNode ID of the cluster node for which you are setting the engineid Default value: -1 Minimum value: 0 Maximum value: 31

show snmp engineId

Displays the ID of the SNMPv3 engine of the Citrix ADC.

Synopsis

show snmp engineId

Arguments

ownerNode ID of the cluster node for which you are setting the engineid Default value: -1 Minimum value: 0 Maximum value: 31

Output

engineID A hexadecimal value of at least 10 characters, uniquely identifying the engineid

defaultEngineID Unique identifier to assign to the SNMPv3 engine. Should be a hexadecimal value with a minimum length of 10 hex characters.

devno count stateflag

unset snmp engineId

Resets the SNMPv3 engine identification (ID) on the Citrix ADC to its default value. The Citrix ADC appliance derives the engine ID from the MAC address of one of its interfaces. Caution: Changing the ID of the SNMPv3 engine invalidates the current SNMP users. You have to reconfigure the SNMP users in the SNMP managers..Refer to the set snmp engineId command for meanings of the arguments.

Synopsis

unset snmp engineId

snmp-group

The following operations can be performed on "snmp-group":

show| set| rm| add|

show snmp group

Displays the settings of all SNMPv3 groups or of the specified SNMPv3 group. To display the settings of all SNMPv3 groups, run the command without any parameters. To display the settings of a particular SNMPv3 group, specify the name of the SNMPv3 group and securityLevel (Security level). The Citrix ADC can have multiple SNMPv3 groups with the same name, differentiated by the securityLevel (Security level) parameter setting.

Synopsis

show snmp group

Arguments

name Name of the SNMPv3 group whose details you want the Citrix ADC to display.

securityLevel Security level of the SNMPv3 group whose details you want the Citrix ADC to display.

Possible values: noAuthNoPriv, authNoPriv, authPriv

Output

readViewName Name of the configured SNMPv3 view that you want to bind to this SNMPv3 group. An SNMPv3 user bound to this group can access the subtrees that are bound to this SNMPv3 view as type INCLUDED, but cannot access the ones that are type EXCLUDED. If the Citrix ADC has multiple SNMPv3 view entries with the same name, all such entries are associated with the SNMPv3 group.

storageType The storage type for this group.

status The status of this group.

devno count stateflag

set snmp group

Modifies the specified parameters of an SNMPv3 group entry on the Citrix ADC.

Synopsis

set snmp group <name> <securityLevel> -readViewName <string>

Arguments

name The name specified in the SNMPv3 group entry that you want to modify. This parameter cannot be modified.

securityLevel Security level required for communication between the Citrix ADC and the SNMPv3 users who belong to the group. Specify one of the following options: noAuthNoPriv. Require neither authentication nor encryption. authNoPriv. Require authentication but no encryption. authPriv. Require authentication and encryption. Note: If you specify authentication, you must specify an encryption algorithm when you assign an SNMPv3 user to the group. If you also specify encryption, you must assign both an authentication and an encryption algorithm for each group member.

Possible values: noAuthNoPriv, authNoPriv, authPriv

readViewName Name of the configured SNMPv3 view that you want to bind to this SNMPv3 group. An SNMPv3 user bound to this group can access the subtrees that are bound to this SNMPv3 view as type INCLUDED, but cannot access the ones that are type EXCLUDED. If the Citrix ADC has multiple SNMPv3 view entries with the same name, all such entries are associated with the SNMPv3 group.

rm snmp group

Removes an SNMPv3 group entry from the Citrix ADC. The appliance can have multiple SNMPv3 groups with the same name, differentiated by the securityLevel (Security level) parameter setting. Therefore, to identify an SNMPv3 group entry that you want to remove, you have to specify both the name and security level of the SNMPv3 group.

Synopsis

rm snmp group <name> <securityLevel>

Arguments

name Name of the SNMPv3 group.

securityLevel Security level of the SNMPv3 group.

Possible values: noAuthNoPriv, authNoPriv, authPriv

add snmp group

Adds an SNMPv3 user group on the Citrix ADC. SNMPv3 groups are logical aggregations of SNMPv3 users. SNMPv3 groups are used to implement access control and define the security levels for the users. You can add a maximum of 1000 SNMPv3 groups to the Citrix ADC appliance.

Synopsis

add snmp group <name> <securityLevel> -readViewName <string>

Arguments

name Name for the SNMPv3 group. Can consist of 1 to 31 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the SNMPv3 group.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose it in double or single quotation marks (for example, "my name" or 'my name').

securityLevel Security level required for communication between the Citrix ADC and the SNMPv3 users who belong to the group. Specify one of the following options: noAuthNoPriv. Require neither authentication nor encryption. authNoPriv. Require authentication but no encryption. authPriv. Require authentication and encryption. Note: If you specify authentication, you must specify an encryption algorithm when you assign an SNMPv3 user to the group. If you also specify

encryption, you must assign both an authentication and an encryption algorithm for each group member.

Possible values: noAuthNoPriv, authNoPriv, authPriv

readViewName Name of the configured SNMPv3 view that you want to bind to this SNMPv3 group. An SNMPv3 user bound to this group can access the subtrees that are bound to this SNMPv3 view as type INCLUDED, but cannot access the ones that are type EXCLUDED. If the Citrix ADC has multiple SNMPv3 view entries with the same name, all such entries are associated with the SNMPv3 group.

snmp-manager

The following operations can be performed on "snmp-manager":

set| unset| rm| show| add|

set snmp manager

Modifies the Domain Resolve Retry parameter of any host-name based SNMP manager configured on the Citrix ADC.

Synopsis

set snmp manager <IPAddress>

Arguments

IPAddress Host name of the SNMP manager for which you want to modify the Domain Resolve Retry parameter.

netmask Subnet mask associated with an IPv4 network address. If the IP address specifies the address or host name of a specific host, accept the default value of 255.255.255.255. Default value: 0xFFFFFFFF

domainResolveRetry Amount of time, in seconds, for which the Citrix ADC waits before sending another DNS query to resolve the host name of the SNMP manager if the last query failed. This parameter is valid for host-name based SNMP managers only. After a query succeeds, the TTL determines the wait time. The minimum and default value is 5. Minimum value: 5 Maximum value: 20939

Example

set snmp manager www.example.com -domainResolveRetry 7

unset snmp manager

Use this command to remove snmp manager settings.Refer to the set snmp manager command for meanings of the arguments.

Synopsis

unset snmp manager <IPAddress> -netmask <netmask> -domainResolveRetry

rm snmp manager

Removes an SNMP manager from the list of managers that are allowed to access the Citrix ADC.

Synopsis

rm snmp manager <IPAddress> ...

Arguments

IPAddress IPv4 or IPv6 address (or IPv4 host name) of the SNMP manager, or the IPv4 network address or IPv6 network prefix of the SNMP managers.

netmask Subnet mask associated with an IPv4 SNMP manager entry. For a specific host, the subnet mask is 255.255.255.255. Default value: 0xFFFFFFFF

Example

rm snmp manager 192.168.1.20 rm snmp manager 192.168.2.16 -netmask 255.255.255.240 rm snmp manager hostnamemanager.com

show snmp manager

Displays configuration information about all SNMP managers on the Citrix ADC, or detailed information about the specified manager.

Synopsis

show snmp manager [<IPAddress>]

Arguments

IPAddress IPv4 or IPv6 address (or IPv4 host name) of the SNMP manager, or the IPv4 network address or IPv6 network prefix of the SNMP managers, about which to display information.

netmask Subnet mask associated with an IPv4-address based SNMP manager entry. If the IP address specifies a specific host (either the IP address or the host name of the SNMP manager), the subnet mask is 255.255.255.255. Default value: 0

Output

IP The resolved IP address of the hostname manager

domain IP address of manager. It will be zero for hostname manager

domainResolveRetry Amount of time, in seconds, for which the Citrix ADC waits before sending another DNS query to resolve the host name of the SNMP manager if the last query failed. This parameter is valid for host-name based SNMP managers only. After a query succeeds, the TTL determines the wait time. The minimum and default value is 5.

devno count stateflag

Example

show snmp manager

add snmp manager

Specifies an SNMP manager to query the Citrix ADC. The added manager complies with SNMP V1, V2, and V3. If you specify one or more SNMP managers, the appliance does not accept SNMP queries from any hosts except the specified SNMP managers. You can specify up to a maximum of 100 IP based SNMP managers or networks and a maximum of 5 host-name based SNMP managers.

Synopsis

add snmp manager <IPAddress> ...

Arguments

IPAddress IP address of the SNMP manager. Can be an IPv4 or IPv6 address. You can instead specify an IPv4 network address or IPv6 network prefix if you want the Citrix ADC to respond to SNMP queries from any device on the specified network. Alternatively, instead of an IPv4 address, you can specify a host name that has been assigned to an SNMP manager. If you do so, you must add a DNS name server that resolves the host name of the SNMP manager to its IP address. Note: The Citrix ADC does not support host names for SNMP managers that have IPv6 addresses.

netmask Subnet mask associated with an IPv4 network address. If the IP address specifies the address or host name of a specific host, accept the default value of 255.255.255.255. Default value: 0xFFFFFFFF

domainResolveRetry Amount of time, in seconds, for which the Citrix ADC waits before sending another DNS query to resolve the host name of the SNMP manager if the last query failed. This parameter is valid for host-name based SNMP managers only. After a query succeeds, the TTL determines the wait time. The minimum and default value is 5. Minimum value: 5 Maximum value: 20939

Example

add snmp manager 192.168.1.20 192.168.2.42 add snmp manager 192.168.2.16 -netmask 255.255.255.240 add snmp manager hostnamemanager.com

snmp-mib

The following operations can be performed on "snmp-mib":

set| unset| show|

set snmp mib

Configures the SNMP agent of the Citrix ADC with information that identifies the appliance, such as the name of the administrator for this Citrix ADC appliance, a name for the appliance, and the location of the appliance. SNMP managers can query the Citrix ADC for this information.

Synopsis

set snmp mib

Arguments

contact Name of the administrator for this Citrix ADC. Along with the name, you can include information on how to contact this person, such as a phone number or an email address. Can consist of 1 to 127 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters.

The following requirement applies only to the Citrix ADC CLI: If the information includes one or more spaces, enclose it in double or single quotation marks (for example, "my contact" or 'my contact'). Default value: "WebMaster (default)"

name Name for this Citrix ADC. Can consist of 1 to 127 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the Citrix ADC appliance.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose it in double or single quotation marks (for example, "my name" or 'my name'). Default value: "NetScaler"

location Physical location of the Citrix ADC. For example, you can specify building name, lab number, and rack number. Can consist of 1 to 127 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters.

The following requirement applies only to the Citrix ADC CLI: If the location includes one or more spaces, enclose it in double or single quotation marks (for example, "my location" or 'my location'). Default value: "POP (default)"

customID Custom identification number for the Citrix ADC. Can consist of 1 to 127 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a custom identification that helps identify the Citrix ADC appliance.

The following requirement applies only to the Citrix ADC CLI: If the ID includes one or more spaces, enclose it in double or single quotation marks (for example, "my ID" or 'my ID'). Default value: "Default"

ownerNode ID of the cluster node for which we are setting the mib. This is a mandatory argument to set snmp mib on CLIP. Default value: -1 Minimum value: 0 Maximum value: 31

unset snmp mib

Use this command to remove snmp mib settings.Refer to the set snmp mib command for meanings of the arguments.

Synopsis

unset snmp mib

show snmp mib

Displays the information that has been configured on the SNMP agent for the purpose of identifying the Citrix ADC, such as the name of the appliance, administrator, and location.

Synopsis

show snmp mib

Arguments

ownerNode ID of the cluster node for which we are setting the mib. This is a mandatory argument to set snmp mib on CLIP. Default value: -1 Minimum value: 0 Maximum value: 31

Output

contact Name of the administrator for this Citrix ADC. Along with the name, you can include information on how to contact this person, such as a phone number or an email address. Can consist of 1 to 127 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters.

The following requirement applies only to the Citrix ADC CLI: If the information includes one or more spaces, enclose it in double or single quotation marks (for example, "my contact" or 'my contact').

name Name for this Citrix ADC. Can consist of 1 to 127 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the Citrix ADC appliance.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose it in double or single quotation marks (for example, "my name" or 'my name').

location Physical location of the Citrix ADC. For example, you can specify building name, lab number, and rack number. Can consist of 1 to 127 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters.

The following requirement applies only to the Citrix ADC CLI: If the location includes one or more spaces, enclose it in double or single quotation marks (for example, "my location" or 'my location').

sysDesc The description of the system.

sysUptime The UP time of the system in 100th of a second.

sysServices The services offered by the system.

sysOID The OID of the system's management system.

customID Custom identification number for the Citrix ADC. Can consist of 1 to 127 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a custom identification that helps identify the Citrix ADC appliance.

The following requirement applies only to the Citrix ADC CLI: If the ID includes one or more spaces, enclose it in double or single quotation marks (for example, "my ID" or 'my ID').

sysDescCL The description of the system from aggregator.

sysUptimeCL The UP time of the system in 100th of a second from aggregator.

devno count stateflag

Example

show snmp mib

snmp-oid

The following operations can be performed on "snmp-oid":

show snmp oid

Displays the corresponding SNMP OIDs for the virtual servers, services, and service groups configured on the Citrix ADC. To display the SNMP OID of all entities of a particular type, such as virtual servers, run the command with only that entity type specified. To display the SNMP of a particular entity, specify the entity type and the entity name.

Synopsis

show snmp oid <entityType>

Arguments

entityType The type of entity whose SNMP OIDs you want to displayType of entity whose SNMP OIDs you want the Citrix ADC to display.

Possible values: VSERVER, SERVICE, SERVICEGROUP

name Name of the entity whose SNMP OID you want the Citrix ADC to display.

Output

snmpOID The snmp oid.

stateflag state flag

devno count

Example

show snmp oid VSERVER vs1

snmp-option

The following operations can be performed on "snmp-option":

set| show| unset|

set snmp option

Enables or disables SNMP options for SNMP SET and SNMP trap logging.

Synopsis

set snmp option

Arguments

snmpset Accept SNMP SET requests sent to the Citrix ADC, and allow SNMP managers to write values to MIB objects that are configured for write access.

Possible values: ENABLED, DISABLED Default value: DISABLED

snmpTrapLogging Log any SNMP trap events (for SNMP alarms in which logging is enabled) even if no trap listeners are configured. With the default setting, SNMP trap events are logged if at least one trap listener is configured on the appliance.

Possible values: ENABLED, DISABLED Default value: DISABLED

partitionNameInTrap Send partition name as a varbind in traps. By default the partition names are not sent as a varbind.

Possible values: ENABLED, DISABLED Default value: DISABLED

snmpTrapLoggingLevel Audit log level of SNMP trap logs. The default value is INFORMATIONAL.

Possible values: EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG Default value: INFORMATIONAL

severityInfoInTrap By default, the severity level info of the trap is not mentioned in the trap message. Enable this option to send severity level of trap as one of the varbind in the trap message.

Possible values: ENABLED, DISABLED Default value: DISABLED

show snmp option

Displays the settings for the following SNMP options: SNMP SET and SNMP trap Logging.

Synopsis

show snmp option

Arguments

Output

snmpset Accept SNMP SET requests sent to the Citrix ADC, and allow SNMP managers to write values to MIB objects that are configured for write access.

snmpTrapLogging Log any SNMP trap events (for SNMP alarms in which logging is enabled) even if no trap listeners are configured. With the default setting, SNMP trap events are logged if at least one trap listener is configured on the appliance.

partitionNameInTrap Send partition name as a varbind in traps. By default the partition names are not sent as a varbind.

snmpTrapLoggingLevel Audit log level of SNMP trap logs. The default value is INFORMATIONAL.

severityInfoInTrap By default, the severity level info of the trap is not mentioned in the trap message. Enable this option to send severity level of trap as one of the varbind in the trap message.

unset snmp option

Use this command to remove snmp option settings.Refer to the set snmp option command for meanings of the arguments.

Synopsis

unset snmp option

snmp-stats

The following operations can be performed on "snmp-stats":

show snmp stats

show snmp stats is an alias for stat snmp Displays the statistics related to SNMP.

Synopsis

show snmp stats - alias for 'stat snmp'

snmp-trap

The following operations can be performed on "snmp-trap":

unset| add| unbind| set| show| rm| bind|

unset snmp trap

Resets the specified parameters to their default settings in a trap-listener entry..Refer to the set snmp trap command for meanings of the arguments.

Synopsis

unset snmp trap <trapClass> <trapDestination>

Example

unset snmp trap generic 192.168.3.4 -version V1 -severity

add snmp trap

Adds an SNMP trap listener. You can configure the Citrix ADC to generate asynchronous events (trap messages) to report abnormal conditions. The trap messages are sent to a remote device (trap listener) to help administrators monitor the appliance and respond promptly to any issues.

Synopsis

add snmp trap <trapClass> <trapDestination> ...

Arguments

trapClass Type of trap messages that the Citrix ADC sends to the trap listener: Generic or the enterprise-specific messages defined in the MIB file.

Possible values: generic, specific

trapDestination IPv4 or the IPv6 address of the trap listener to which the Citrix ADC is to send SNMP trap messages.

version SNMP version, which determines the format of trap messages sent to the trap listener. This setting must match the setting on the trap listener. Otherwise, the listener drops the trap messages.

Possible values: V1, V2, V3 Default value: V2

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

destPort UDP port at which the trap listener listens for trap messages. This setting must match the setting on the trap listener. Otherwise, the listener drops the trap messages. Default value: 162 Minimum value: 1 Maximum value: 65534

communityName Password (string) sent with the trap messages, so that the trap listener can authenticate them. Can include 1 to 31 uppercase or lowercase letters, numbers, and hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) characters. You must specify the same community string on the trap listener device. Otherwise, the trap listener drops the trap messages.

The following requirement applies only to the Citrix ADC CLI: If the string includes one or more spaces, enclose the name in double or single quotation marks (for example, "my string" or 'my string').

srcIP IPv4 or IPv6 address that the Citrix ADC inserts as the source IP address in all SNMP trap messages that it sends to this trap listener. By default this is the appliance's NSIP or NSIP6 address, but you can specify an IPv4 MIP or SNIP/SNIP6 address. In cluster setup, the default

value is the individual node's NSIP, but it can be set to CLIP or Striped SNIP address. In non default partition, this parameter must be set to the SNIP/SNIP6 address.

severity Severity level at or above which the Citrix ADC sends trap messages to this trap listener. The severity levels, in increasing order of severity, are Informational, Warning, Minor, Major, Critical. This parameter can be set for trap listeners of type SPECIFIC only. The default is to send all levels of trap messages. Important: Trap messages are not assigned severity levels unless you specify severity levels when configuring SNMP alarms.

Possible values: Critical, Major, Minor, Warning, Informational Default value: Unknown

allPartitions Send traps of all partitions to this destination.

Possible values: ENABLED, DISABLED Default value: DISABLED

unbind snmp trap

Unbind snmp user to a V3 trap

Synopsis

unbind snmp trap <trapClass> <trapDestination> -userName <string>

Arguments

trapClass Type of trap messages that the Citrix ADC sends to the trap listener: Generic or the enterprise-specific messages defined in the MIB file.

Possible values: generic, specific

trapDestination IPv4 or the IPv6 address of the trap listener to which the Citrix ADC is to send SNMP trap messages.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

version SNMP version, which determines the format of trap messages sent to the trap listener. This setting must match the setting on the trap listener. Otherwise, the listener drops the trap messages.

Possible values: V1, V2, V3 Default value: V3

userName Name of the SNMP user that will send the SNMPv3 traps.

set snmp trap

Modifies the specified parameters in a trap-listener entry.

Synopsis

set snmp trap <trapClass> <trapDestination>

Arguments

trapClass Type of trap specified in the trap-listener entry. Because this parameter is used for identifying the trap listener entry, it cannot be modified after the entry has been created.

Possible values: generic, specific

trapDestination IPv4 or the IPv6 address of the trap listener to which the Citrix ADC is to send SNMP trap messages.

version SNMP version, which determines the format of trap messages sent to the trap listener. This setting must match the setting on the trap listener. Otherwise, the listener drops the trap messages.

Possible values: V1, V2, V3 Default value: V2

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

destPort UDP port at which the trap listener listens for trap messages. This setting must match the setting on the trap listener. Otherwise, the listener drops the trap messages. Default value: 162 Minimum value: 1 Maximum value: 65534

communityName Password (string) sent with the trap messages, so that the trap listener can authenticate them. Can include 1 to 31 uppercase or lowercase letters, numbers, and hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) characters. You must specify the same community string on the trap listener device. Otherwise, the trap listener drops the trap messages.

The following requirement applies only to the Citrix ADC CLI: If the string includes one or more spaces, enclose the name in double or single quotation marks (for example, "my string" or 'my string').

srcIP IPv4 or IPv6 address that the Citrix ADC inserts as the source IP address in all SNMP trap messages that it sends to this trap listener. By default this is the appliance's NSIP or NSIP6 address, but you can specify an IPv4 MIP or SNIP/SNIP6 address. In cluster setup, the default value is the individual node's NSIP, but it can be set to CLIP or Striped SNIP address. In non default partition, this parameter must be set to the SNIP/SNIP6 address.

severity Severity level at or above which the Citrix ADC sends trap messages to this trap listener. The severity levels, in increasing order of severity, are Informational, Warning, Minor, Major, Critical. This parameter can be set for trap listeners of type SPECIFIC only. The default is to send all levels of trap messages. Important: Trap messages are not assigned severity levels unless you specify severity levels when configuring SNMP alarms.

Possible values: Critical, Major, Minor, Warning, Informational Default value: Unknown

allPartitions Send traps of all partitions to this destination.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set snmp trap generic 192.168.3.4 -version V1 -severity Critical

show snmp trap

Displays the settings of all trap listeners or of the specified trap listener. To display the settings of all the trap listeners, run the command without any parameters. To display the settings of a particular trap listener, specify the trapClass (Trap Type) and trapDestination (IP Address) of the trap listener.

Synopsis

show snmp trap [<trapClass> <trapDestination>]

Arguments

trapClass Trap type specified in the trap listener entry.

Possible values: generic, specific

trapDestination IP address specified in the trap listener entry.

version The SNMP version of the trap specified in the trap listener entry.

Possible values: V1, V2, V3

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

Output

destPort The destination port of the SNMP trap.

communityName Password (string) sent with the trap messages, so that the trap listener can authenticate them. Can include 1 to 31 uppercase or lowercase letters, numbers, and hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) characters. You must specify the same community string on the trap listener device. Otherwise, the trap listener drops the trap messages.

The following requirement applies only to the Citrix ADC CLI: If the string includes one or more spaces, enclose the name in double or single quotation marks (for example, "my string" or 'my string').

srcIP The source IP of the SNMP trap to be sent.

severity The minimum severity of traps to be sent to this destination.

allPartitions Send traps of all partitions to this destination.

userName Name of the SNMP user that will send the SNMPv3 traps.

securityLevel Security level of the SNMPv3 trap.

stateflag devno count

Example

show snmp trap

rm snmp trap

Removes a trap listener entry from the Citrix ADC.

Synopsis

rm snmp trap <trapClass> <trapDestination> ...

Arguments

trapClass Trap type specified in the trap listener entry that you want to remove.

Possible values: generic, specific

trapDestination IP address of the trap listener specified in the trap listener entry that you want to remove.

version Version of the trap specified in the trap listener entry that you want to remove.

Possible values: V1, V2, V3 Default value: V2

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

bind snmp trap

Binds an SNMPv3 trap to an SNMP user.

Synopsis

bind snmp trap <trapClass> <trapDestination> (-userName <string>)

Arguments

trapClass Type of trap messages that the Citrix ADC sends to the trap listener: Generic or the enterprise-specific messages defined in the MIB file.

Possible values: generic, specific

trapDestination IPv4 or the IPv6 address of the trap listener to which the Citrix ADC is to send SNMP trap messages.

td Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value: 0 Maximum value: 4094

version SNMP version, which determines the format of trap messages sent to the trap listener. This setting must match the setting on the trap listener. Otherwise, the listener drops the trap messages.

Possible values: V1, V2, V3 Default value: V3

userName Name of the SNMP user that will send the SNMPv3 traps.

securityLevel Security level of the SNMPv3 trap.

Possible values: noAuthNoPriv, authNoPriv, authPriv Default value: authNoPriv,

snmp-user

The following operations can be performed on "snmp-user":

add| show| rm| set| unset|

add snmp user

Adds an SNMPv3 user who can send SNMP queries to the Citrix ADC. You can add a maximum of 1000 SNMPv3 users.

Synopsis

add snmp user <name> -group <string> [-authType (MD5 | SHA) {-authPasswd }]

Arguments

name Name for the SNMPv3 user. Can consist of 1 to 31 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose it in double or single quotation marks (for example, "my user" or 'my user').

group Name of the configured SNMPv3 group to which to bind this SNMPv3 user. The access rights (bound SNMPv3 views) and security level set for this group are assigned to this user.

authType Authentication algorithm used by the Citrix ADC and the SNMPv3 user for authenticating the communication between them. You must specify the same authentication algorithm when you configure the SNMPv3 user in the SNMP manager.

Possible values: MD5, SHA

authPasswd Plain-text pass phrase to be used by the authentication algorithm specified by the authType (Authentication Type) parameter. Can consist of 1 to 31 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters.

The following requirement applies only to the Citrix ADC CLI: If the pass phrase includes one or more spaces, enclose it in double or single quotation marks (for example, "my phrase" or 'my phrase').

privType Encryption algorithm used by the Citrix ADC and the SNMPv3 user for encrypting the communication between them. You must specify the same encryption algorithm when you configure the SNMPv3 user in the SNMP manager.

Possible values: DES, AES

privPasswd Encryption key to be used by the encryption algorithm specified by the privType (Encryption Type) parameter. Can consist of 1 to 31 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters.

The following requirement applies only to the Citrix ADC CLI: If the key includes one or more spaces, enclose it in double or single quotation marks (for example, "my key" or 'my key').

show snmp user

Displays the settings of all SNMPv3 users or of the specified SNMPv3 user. To display the settings of all the SNMPv3 users, run the command without any parameters. To display the settings of a particular SNMPv3 user, specify the name of the SNMPv3 user.

Synopsis

show snmp user

Arguments

name Name of the SNMPv3 user whose details you want the Citrix ADC to display.

Output

group Name of the configured SNMPv3 group to which to bind this SNMPv3 user. The access rights (bound SNMPv3 views) and security level set for this group are assigned to this user.

authType Authentication algorithm used by the Citrix ADC and the SNMPv3 user for authenticating the communication between them. You must specify the same authentication algorithm when you configure the SNMPv3 user in the SNMP manager.

authPasswd Plain-text pass phrase to be used by the authentication algorithm specified by the authType (Authentication Type) parameter. Can consist of 1 to 31 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters.

The following requirement applies only to the Citrix ADC CLI: If the pass phrase includes one or more spaces, enclose it in double or single quotation marks (for example, "my phrase" or 'my phrase').

privType Encryption algorithm used by the Citrix ADC and the SNMPv3 user for encrypting the communication between them. You must specify the same encryption algorithm when you configure the SNMPv3 user in the SNMP manager.

privPasswd Encryption key to be used by the encryption algorithm specified by the privType (Encryption Type) parameter. Can consist of 1 to 31 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters.

The following requirement applies only to the Citrix ADC CLI: If the key includes one or more spaces, enclose it in double or single quotation marks (for example, "my key" or 'my key').

engineID The context engine ID of the user.

storageType The storage type for this user.

status The status of this user.

devno count stateflag

rm snmp user

Removes an SNMPv3 user entry from the Citrix ADC.

Synopsis

rm snmp user <name>

Arguments

name Name of the SNMPv3 user.

set snmp user

Modifies the specified parameters of an SNMPv3 user entry on the Citrix ADC.

Synopsis

set snmp user <name>

Arguments

name Name specified in the SNMPv3 user entry that you want to modify. Because this parameter is used for identifying the SNMPv3 user entry, it cannot be modified after the entry has been created.

group Name of the configured SNMPv3 group to which to bind this SNMPv3 user. The access rights (bound SNMPv3 views) and security level set for this group are assigned to this user.

authType Authentication algorithm used by the Citrix ADC and the SNMPv3 user for authenticating the communication between them. You must specify the same authentication algorithm when you configure the SNMPv3 user in the SNMP manager.

Possible values: MD5, SHA

authPasswd Plain-text pass phrase to be used by the authentication algorithm specified by the authType (Authentication Type) parameter. Can consist of 1 to 31 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters.

The following requirement applies only to the Citrix ADC CLI: If the pass phrase includes one or more spaces, enclose it in double or single quotation marks (for example, "my phrase" or 'my phrase').

privType Encryption algorithm used by the Citrix ADC and the SNMPv3 user for encrypting the communication between them. You must specify the same encryption algorithm when you configure the SNMPv3 user in the SNMP manager.

Possible values: DES, AES

privPasswd Encryption key to be used by the encryption algorithm specified by the privType (Encryption Type) parameter. Can consist of 1 to 31 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters.

The following requirement applies only to the Citrix ADC CLI: If the key includes one or more spaces, enclose it in double or single quotation marks (for example, "my key" or 'my key').

unset snmp user

Resets the specified parameters of an SNMPv3 user entry to their default settings..Refer to the set snmp user command for meanings of the arguments.

Synopsis

unset snmp user <name> (-authType | -privType)

snmp-view

The following operations can be performed on "snmp-view":

show| add| set| rm|

show snmp view

Displays the settings of all SNMPv3 views or of the specified SNMPv3 view. To display the settings of all the SNMPv3 views, run the command without any parameters. To display the settings of a particular SNMPv3 view, specify the name of the SNMPv3 view and subtree (the associated subtree of the MIB). The Citrix ADC can have multiple SNMPv3 views with the same name, differentiated by the subtree parameter settings.

Synopsis

show snmp view [<name>]

Arguments

name Name of the SNMPv3 view.

subtree A MIB subtree of the SNMPv3 view.

Output

type The type of sutree.

storageType The storage type for this view.

status The status of this view.

devno count stateflag

add snmp view

Adds an SNMPv3 view. Used to implement access control for the SNMPv3 user, SNMPv3 views restrict user access to specific portions of the MIB. The Citrix ADC can have multiple SNMPv3 views with the same name, differentiated by subtree parameter settings. You can add a maximum of 1000 SNMPv3 views.

Synopsis

add snmp view <name> <subtree> -type (included | excluded)

Arguments

name Name for the SNMPv3 view. Can consist of 1 to 31 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the SNMPv3 view.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose it in double or single quotation marks (for example, "my view" or 'my view').

subtree A particular branch (subtree) of the MIB tree that you want to associate with this SNMPv3 view. You must specify the subtree as an SNMP OID.

type Include or exclude the subtree, specified by the subtree parameter, in or from this view. This setting can be useful when you have included a subtree, such as A, in an SNMPv3 view and you want to exclude a specific subtree of A, such as B, from the SNMPv3 view.

Possible values: included, excluded

set snmp view

Modifies the type (Type) parameter of an SNMPv3 view configured on the Citrix ADC.

Synopsis

set snmp view <name> <subtree> -type (included | excluded)

Arguments

name The name specified in the SNMPv3 view entry. This parameter cannot be modified.

subtree A MIB subtree of the SNMPv3 view entry. This parameter cannot be modified.

type Include or exclude the subtree, specified by the subtree parameter, in or from this view. This setting can be useful when you have included a subtree, such as A, in an SNMPv3 view and you want to exclude a specific subtree of A, such as B, from the SNMPv3 view.

Possible values: included, excluded

rm snmp view

Removes an SNMPv3 view entry from the Citrix ADC. The appliance can have multiple SNMPv3 views with the same name, differentiated by the subtree parameter setting. Therefore, to identify an SNMPv3 group subtree that you want to remove, you have to specify both the name and subtree of the SNMPv3 view.

Synopsis

rm snmp view <name> <subtree>

Arguments

name Name of the SNMPv3 view. Note: If multiple views have the same name, specify the subtree to identify the view to be removed.

subtree A MIB subtree of the SNMPv3 view.

snmp

The following operations can be performed on "snmp":

stat snmp

Display the statistics related to SNMP.

Synopsis

stat snmp

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

SNMP packets received (PktsRx) SNMP packets received.

SNMP packets sent (PktsTx) SNMP packets transmitted.

Get requests receieved (GetReqRx) SNMP Get-Request PDUs that have been accepted and processed.

Get-next requests receieved (GtNextRx) SNMP Get-Next PDUs that have been accepted and processed.

Get-bulk requests received (GtBulkRx) SNMP Get-Bulk PDUs that have been accepted and processed.

Responses sent (RspTx) SNMP Get-Response PDUs that have been generated by the Citrix ADC.

Traps messages sent (TrapsTx) SNMP Trap PDUs that have been generated by the Citrix ADC.

Requests dropped (ReqDrop) SNMP requests dropped.

ASN.1/BER errors in requests (PrsErrRx) Number of ASN.1 or BER errors encountered when decoding received SNMP Messages.

Unsupported SNMP version (UnkVrsRx) Number of SNMP messages received, which were for an unsupported SNMP version.

Unknown community name (UnkCNRx) SNMP messages received, which used an SNMP community name not known to the Citrix ADC.

No permission on community (BadCURx) The total number of SNMP Messages received that represented an SNMP operation which was not allowed by the SNMP community named in the Message.

Unsupported security level (UnkSecLv) SNMP packets that were dropped because they requested a security level that was unknown to the Citrix ADC or otherwise unavailable.

Not in time window (NtTimeWd) SNMP packets that were dropped because they appeared outside of the authoritative SNMP engine's window.

Unknown user name (UnkUser) SNMP packets that were dropped because they referenced a user that was not known to the SNMP engine.

Unknown engine Id (UnkEngId) SNMP packets that were dropped because they referenced an SNMP engine ID that was not known to the Citrix ADC.

Wrong digest value (WrgDgst) SNMP packets that were dropped because they did not contain the expected digest value.

Decryption errors (DcrptErr) SNMP packets that were dropped because they could not be decrypted.

Example

stat snmp

spillover

spillover-action

The following operations can be performed on "spillover-action":

show| rename| rm| add|

show spillover action

Displaying spillover actions

Synopsis

show spillover action

Arguments

name Name of the spillover action.

Output

action Spillover action. Currently only type SPILLOVER is supported

builtin Flag to determine whether compression is default or not

feature The feature to be checked while applying this config

gslbBindings Number of times action is used in a policy bound to a gslb vserver

devno count stateflag

rename spillover action

Renames a spillover action.

Synopsis

rename spillover action <name>@ <newName>@

Arguments

name Existing name of the action.

newName New name for the spillover action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Choose a name that can be correlated with the function that the action performs.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

Example

rename spillover policy oldname newname

rm spillover action

Removes a spillover policy.

Synopsis

rm spillover action <name>

Arguments

name Name of the spillover action.

add spillover action

Creating spillover action

Synopsis

add spillover action <name> -action SPILLOVER

Arguments

name Name of the spillover action.

action Spillover action. Currently only type SPILLOVER is supported

Possible values: SPILLOVER

Spillover

The entities on which you can perform NetScaler CLI operations:

- spillover-action
- spillover-policy

spillover-policy

The following operations can be performed on "spillover-policy":

add| show| stat| rm| rename| unset| set|

add spillover policy

Add a spillover policy. SPILLOVER policies that can be added are based on vserver expressions.

Synopsis

add spillover policy <name> -rule <expression> -action <string>

Arguments

name Name of the spillover policy.

rule Expression to be used by the spillover policy.

action Action for the spillover policy. Action is created using add spillover action command

comment Any comments that you might want to associate with the spillover policy.

Example

add spillover policy pol1 -rule "SYS.VSERVER("abc").ACTIVESERVICES.LE(2) -action act1 add spillover policy pol2 -rule "SYS.VSERVER("abc").CONNECTIONS.GT(500) -action act2"

show spillover policy

Displaying the policy-related information.

Synopsis

show spillover policy

Arguments

name Name of the spillover policy.

Output

stateflag rule Expression to be used by the spillover policy.

action Action for the spillover policy. Action is created using add spillover action command

boundTo The name of the entity to which the policy is bound.

hits The number of times the policy has been hit.

undefHits Number of policy UNDEF hits.

activePolicy Indicates whether policy is bound or not.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

comment Any comments that you might want to associate with the spillover policy.

builtin Flag to determine if compression policy is builtin or not

feature The feature to be checked while applying this config

gslbBindings Number of times the policy bound to a gslb vserver

type devno count

stat spillover policy

Displays statistics for all spillover policies currently configured on the Citrix ADC, or detailed statistics for the specified policy.

Synopsis

stat spillover policy

Arguments

name Name of the spillover policy for which to show detailed statistics.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Policy undef hits (Undefhits) Number of undef hits on the policy

rm spillover policy

Removes a spillover policy.

Synopsis

rm spillover policy <name>

Arguments

name Name of the spillover policy.

rename spillover policy

Renames a spillover policy.

Synopsis

rename spillover policy <name>@ <newName>@

Arguments

name Existing name of the policy.

newName New name for the spillover policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Choose a name that reflects the function that the policy performs.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

Example

rename spillover policy oldname newname

unset spillover policy

Use this command to remove spillover policy settings.Refer to the set spillover policy command for meanings of the arguments.

Synopsis

unset spillover policy <name> -comment

set spillover policy

Used to change the expression or other parameters of an existing policy.

Synopsis

set spillover policy <name>

Arguments

name Name of the spillover policy.

rule Expression to be used by the spillover policy.

action Action for the spillover policy. Action is created using add spillover action command

comment Any comments that you might want to associate with the spillover policy.

Example

set spillover policy pol1 -rule "SYS.VSERVER("abc").ACTIVESERVICS.LE(1)" set spillover policy pol2 -action act4"

ssl

ssl-action

The following operations can be performed on "ssl-action":

show| add| rm|

show ssl action

Displays information about all the SSL actions configured on the appliance, or displays detailed information about the specified SSL action.

Synopsis

show ssl action

Arguments

name Name of the SSL action for which to show detailed information.

Output

stateflag clientAuth Perform client certificate authentication.

clientCertVerification Client certificate verification is mandatory or optional.

clientCert Insert the entire client certificate into the HTTP header of the request being sent to the web server. The certificate is inserted in ASCII (PEM) format.

certHeader clientCertSerialNumber Insert the entire client serial number into the HTTP header of the request being sent to the web server.

certSerialHeader clientCertSubject Insert the client certificate subject, also known as the distinguished name (DN), into the HTTP header of the request being sent to the web server.

certSubjectHeader clientCertHash Insert the certificate's signature into the HTTP header of the request being sent to the web server. The signature is the value extracted directly from the X.509 certificate signature field. All X.509 certificates contain a signature field.

certHashHeader clientCertFingerprint Insert the certificate's fingerprint into the HTTP header of the request being sent to the web server. The fingerprint is derived by computing the specified hash value (SHA256, for example) of the DER-encoding of the client certificate.

certFingerprintHeader certFingerprintDigest clientCertIssuer Insert the certificate issuer details into the HTTP header of the request being sent to the web server.

certIssuerHeader sessionID Insert the SSL session ID into the HTTP header of the request being sent to the web server. Every SSL connection that the client and the Citrix ADC share has a unique ID that identifies the specific connection.

sessionIDHeader cipher Insert the cipher suite that the client and the Citrix ADC negotiated for the SSL session into the HTTP header of the request being sent to the web server. The appliance inserts the cipher-suite name, SSL protocol, export or non-export string, and cipher strength bit, depending on the type of browser connecting to the SSL virtual server or service (for example, Cipher-Suite: RC4- MD5 SSLv3 Non-Export 128-bit).

cipherHeader OWASupport If the appliance is in front of an Outlook Web Access (OWA) server, insert a special header field, FRONT-END-HTTPS: ON, into the HTTP requests going to the OWA server. This header communicates to the server that the transaction is HTTPS and not HTTP.

forward This action takes an argument a vserver name, to this vserver one will be able to forward all the packets.

caCertGrpName This action will allow to pick CA(s) from the specific CA group, to verify the client certificate.

clientCertNotBefore Insert the date from which the certificate is valid into the HTTP header of the request being sent to the web server. Every certificate is configured with the date and time from which it is valid.

certNotBeforeHeader clientCertNotAfter Insert the date of expiry of the certificate into the HTTP header of the request being sent to the web server. Every certificate is configured with the date and time at which the certificate expires.

certNotAfterHeader hits The number of times the action has been taken.

undefHits The number of times the action resulted in UNDEF.

referenceCount The number of references to the action.

description Description of the action

flags ssllogProfile The name of the ssllogprofile.

builtin Flag to determine whether ssl action is built-in or not

feature The feature to be checked while applying this config

devno count

Example

show ssl action 1 Configured SSL action: 1)

```
    Name: certInsert_act

    Data Insertion Action:

    Cert Header: ENABLED            Cert Tag: CERT
```

add ssl action

Creates a new SSL action. An SSL action defines SSL settings that you can apply to the selected requests. You associate an action with one or more policies. Data in client connection requests or responses is compared to a rule (expression) specified in the policy, and the action is applied to connections that match the rule.

Synopsis

add ssl action <name> ((-clientAuth (DOCLIENTAUTH | NOCLIENTAUTH)) | -forward <string> | -caCertGrpName <string>)

Arguments

name Name for the SSL action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

clientAuth Perform client certificate authentication.

Possible values: DOCLIENTAUTH, NOCLIENTAUTH

clientCertVerification Client certificate verification is mandatory or optional.

Possible values: Mandatory, Optional Default value: Mandatory

ssllogProfile The name of the ssllogprofile.

clientCert Insert the entire client certificate into the HTTP header of the request being sent to the web server. The certificate is inserted in ASCII (PEM) format.

Possible values: ENABLED, DISABLED

certHeader Name of the header into which to insert the client certificate.

clientCertSerialNumber Insert the entire client serial number into the HTTP header of the request being sent to the web server.

Possible values: ENABLED, DISABLED

certSerialHeader Name of the header into which to insert the client serial number.

clientCertSubject Insert the client certificate subject, also known as the distinguished name (DN), into the HTTP header of the request being sent to the web server.

Possible values: ENABLED, DISABLED

certSubjectHeader Name of the header into which to insert the client certificate subject.

clientCertHash Insert the certificate's signature into the HTTP header of the request being sent to the web server. The signature is the value extracted directly from the X.509 certificate signature field. All X.509 certificates contain a signature field.

Possible values: ENABLED, DISABLED

certHashHeader Name of the header into which to insert the client certificate signature (hash).

clientCertFingerprint Insert the certificate's fingerprint into the HTTP header of the request being sent to the web server. The fingerprint is derived by computing the specified hash value (SHA256, for example) of the DER-encoding of the client certificate.

Possible values: ENABLED, DISABLED

certFingerprintHeader Name of the header into which to insert the client certificate fingerprint.

certFingerprintDigest Digest algorithm used to compute the fingerprint of the client certificate.

Possible values: SHA1, SHA224, SHA256, SHA384, SHA512

clientCertIssuer Insert the certificate issuer details into the HTTP header of the request being sent to the web server.

Possible values: ENABLED, DISABLED

certIssuerHeader Name of the header into which to insert the client certificate issuer details.

sessionID Insert the SSL session ID into the HTTP header of the request being sent to the web server. Every SSL connection that the client and the Citrix ADC share has a unique ID that identifies the specific connection.

Possible values: ENABLED, DISABLED

sessionIDHeader Name of the header into which to insert the Session ID.

cipher Insert the cipher suite that the client and the Citrix ADC negotiated for the SSL session into the HTTP header of the request being sent to the web server. The appliance inserts the cipher-suite name, SSL protocol, export or non-export string, and cipher strength bit, depending on the type of browser connecting to the SSL virtual server or service (for example, Cipher-Suite: RC4-MD5 SSLv3 Non-Export 128-bit).

Possible values: ENABLED, DISABLED

cipherHeader Name of the header into which to insert the name of the cipher suite.

clientCertNotBefore Insert the date from which the certificate is valid into the HTTP header of the request being sent to the web server. Every certificate is configured with the date and time from which it is valid.

Possible values: ENABLED, DISABLED

certNotBeforeHeader Name of the header into which to insert the date and time from which the certificate is valid.

clientCertNotAfter Insert the date of expiry of the certificate into the HTTP header of the request being sent to the web server. Every certificate is configured with the date and time at which the certificate expires.

Possible values: ENABLED, DISABLED

certNotAfterHeader Name of the header into which to insert the certificate's expiry date.

OWASupport If the appliance is in front of an Outlook Web Access (OWA) server, insert a special header field, FRONT-END-HTTPS: ON, into the HTTP requests going to the OWA server. This header communicates to the server that the transaction is HTTPS and not HTTP.

Possible values: ENABLED, DISABLED

forward This action takes an argument a vserver name, to this vserver one will be able to forward all the packets.

caCertGrpName This action will allow to pick CA(s) from the specific CA group, to verify the client certificate.

Example

add ssl action certInsert_act -clientCert ENABLED -certHeader CERT

rm ssl action

Removes the specified SSL action.

Synopsis

rm ssl action <name>

Arguments

name Name of the SSL action to remove.

Example

rm ssl action certInsert_act

ssl-caCertGroup

The following operations can be performed on "ssl-caCertGroup":

unbind| rm| show| bind| add|

unbind ssl caCertGroup

Unbinds the specified CA certificates from the group.

Synopsis

unbind ssl caCertGroup <caCertGroupName> <certkeyName>

Arguments

caCertGroupName Name given to the CA certificate group. The name will be used to add the CA certificates to the group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

certkeyName Name of the certificate-key pair.

Example

unbind ssl cacertgroup <cacertgroup_name> <cacertkey_name>

rm ssl caCertGroup

Deletes the specified CA certificate group.

Synopsis

rm ssl caCertGroup <caCertGroupName>

Arguments

caCertGroupName Name given to the CA certificate group. The name will be used to add the CA certificates to the group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

Example

rm ssl cacertgroup <cacertgroup_name>

show ssl caCertGroup

Lists information about either all CA certificate groups or the specified CA certificate group.

Synopsis

show ssl caCertGroup

Arguments

caCertGroupName Name of the CA certificate group for which to show detailed information.

Output

stateflag caCertGroupReferences Count for ssl actions referring to this ca certificate group.

certkeyName Name for the certkey added to the Citrix ADC. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the certificate-key pair is created.The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cert" or 'my cert').

ocspCheck The state of the OCSP check parameter. (Mandatory/Optional)

crlCheck The state of the CRL check parameter. (Mandatory/Optional)

devno count

Example

1. show ssl cacertgroup <cacertgroup_name>
2. show ssl cacertgroup

bind ssl caCertGroup

Binds the specified CA certificates to the group.

Synopsis

bind ssl caCertGroup <caCertGroupName> (<certkeyName>)

Arguments

caCertGroupName Name given to the CA certificate group. The name will be used to add the CA certificates to the group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

certkeyName Name of the certificate-key pair.

crlCheck Rule to use for the CRL corresponding to the CA certificate during client authentication. Available settings function as follows:

- MANDATORY - Deny SSL clients if the CRL is missing or expired, or the Next Update date is in the past, or the CRL is incomplete.
- OPTIONAL - Allow SSL clients if the CRL is missing or expired, or the Next Update date is in the past, or the CRL is incomplete, but deny if the client certificate is revoked in the CRL.

Possible values: Mandatory, Optional Default value: CRLCHECK_OPTIONAL

ocspCheck Rule to use for the OCSP responder associated with the CA certificate during client authentication. If MANDATORY is specified, deny all SSL clients if the OCSP check fails because of connectivity issues with the remote OCSP server, or any other reason that prevents the OCSP check. With the OPTIONAL setting, allow SSL clients even if the OCSP check fails except when the client certificate is revoked.

Possible values: Mandatory, Optional

Example

bind ssl cacertgroup <cacertgroup_name> <cacertkey_name>

add ssl caCertGroup

Creates a new CA certificate group.

Synopsis

add ssl caCertGroup <caCertGroupName>

Arguments

caCertGroupName Name given to the CA certificate group. The name will be used to add the CA certificates to the group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

Example

add ssl cacertgroup

ssl-cert

The following operations can be performed on "ssl-cert":

create ssl cert

Generates a signed X509 Certificate.

Synopsis

create ssl cert <certFile> <reqFile> <certType>

Arguments

certFile Name for and, optionally, path to the generated certificate file. /nsconfig/ssl/ is the default path. Maximum value: 63

reqFile Name for and, optionally, path to the certificate-signing request (CSR). /nsconfig/ssl/ is the default path. Maximum value: 63

certType Type of certificate to generate. Specify one of the following:

- ROOT_CERT - Self-signed Root-CA certificate. You must specify the key file name. The generated Root-CA certificate can be used for signing end-user client or server certificates or to create Intermediate-CA certificates.
- INTM_CERT - Intermediate-CA certificate.
- CLNT_CERT - End-user client certificate used for client authentication.
- SRVR_CERT - SSL server certificate used on SSL servers for end-to-end encryption.

Possible values: ROOT_CERT, INTM_CERT, CLNT_CERT, SRVR_CERT

keyFile Name for and, optionally, path to the private key. You can either use an existing RSA or DSA key that you own or create a new private key on the Citrix ADC. This file is required only when creating a self-signed Root-CA certificate. The key file is stored in the /nsconfig/ssl directory by default. If the input key specified is an encrypted key, you are prompted to enter the PEM pass phrase that was used for encrypting the key. Maximum value: 63

keyform Format in which the key is stored on the appliance.

Possible values: DER, PEM Default value: PEM

PEMPassPhrase days Number of days for which the certificate will be valid, beginning with the time and day (system time) of creation. Default value: 365 Minimum value: 1 Maximum value: 3650

subjectAltName Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field. These values are called "Subject Alternative Names" (SAN). Names include:

1. Email addresses
2. IP addresses
3. URIs
4. DNS names (This is usually also provided as the Common Name RDN within the Subject field of the main certificate.)
5. directory names (alternative Distinguished Names to that given in the Subject)

certForm Format in which the certificate is stored on the appliance.

Possible values: DER, PEM Default value: PEM

CAcert Name of the CA certificate file that issues and signs the Intermediate-CA certificate or the end-user client and server certificates. Maximum value: 63

CAcertForm Format of the CA certificate.

Possible values: DER, PEM Default value: PEM

CAkey Private key, associated with the CA certificate that is used to sign the Intermediate-CA certificate or the end-user client and server certificate. If the CA key file is password protected, the user is prompted to enter the pass phrase that was used to encrypt the key. Maximum value: 63

CAkeyForm Format for the CA certificate.

Possible values: DER, PEM Default value: PEM

CAserial Serial number file maintained for the CA certificate. This file contains the serial number of the next certificate to be issued or signed by the CA. If the specified file does not exist, a new file is created, with /nsconfig/ssl/ as the default path. If you do not specify a proper path for the existing serial file, a new serial file is created. This might change the certificate serial numbers assigned by the CA certificate to each of the certificates it signs. Maximum value: 63

Example

1. create ssl cert /nsconfig/ssl/root_cert.pem /nsconfig/ssl/root_csr.pem ROOT_CERT -keyFile /nsconfig/ssl/root_key.pem -days 1000 The above example creates a self signed Root-CA certificate.

2. create ssl cert /nsconfig/ssl/server_cert.pem /nsconfig/ssl/server_csr.pem SRVR_CERT -CAcert /nsconfig/ssl/root_cert.pem -CAkey /nsconfig/ssl/root_key.pem -CAserial /nsconfig/ssl/root.srl The above example creates a Server certificate which is signed by the Root-CA certificate: root_cert.pem

Related Commands

- add ssl certkey

ssl-certBundle

The following operations can be performed on "ssl-certBundle":

import| show| export| rm| apply|

import ssl certBundle

Imports a certificate bundle to the Citrix ADC, assigns it a name, and stores it.

Synopsis

import ssl certBundle <name> <src>

Arguments

name Name to assign to the imported certificate bundle. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

src URL specifying the protocol, host, and path, including file name, to the certificate bundle to be imported or exported. For example, http://www.example.com/cert_bundle_file. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

Example

import ssl certbundle my-certbundle http://www.example.com/cert_bundle

show ssl certBundle

Displays a list of all the imported certificate bundle objects on the Citrix ADC.

Synopsis

show ssl certBundle

Arguments

Output

name Name to assign to the imported certificate bundle. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

inUse src URL specifying the protocol, host, and path, including file name, to the certificate bundle to be imported or exported. For example, http://www.example.com/cert_bundle_file. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

devno count stateflag

Example

show ssl certbundle

export ssl certBundle

Exports a certificate bundle from one appliance to another for backup or editing purpose.

Synopsis

export ssl certBundle <name> <src>

Arguments

name Name to assign to the imported certificate bundle. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

src URL specifying the protocol, host, and path, including file name, to the certificate bundle to be imported or exported. For example, http://www.example.com/cert_bundle_file. NOTE: The import

fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

Example

export ssl certbundle my-certbundle

rm ssl certBundle

Deletes the specified certificate bundle.

Synopsis

rm ssl certBundle <name>

Arguments

name Name to assign to the imported certificate bundle. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

Example

rm ssl certbundle my-certbundle

apply ssl certBundle

Applies the specified CA certificate bundle and the device starts using the applied CA bundle to validate the server certificate. Use 'apply ssl certBundle DEFAULT' to restore the default CA certificate bundle.

Synopsis

apply ssl certBundle <name>

Arguments

name Name to assign to the imported certificate bundle. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

Example

apply ssl certbundle my-certbundle

ssl-certChain

The following operations can be performed on "ssl-certChain":

show ssl certChain

Display all the certificates attached to this particular certificate.

Synopsis

show ssl certChain

Arguments

CertKeyName Name of the Certificate

Output

linkCertKeyName Name of the Linked Certificate

IsLinked Used to find if certificate is linked

IsCA Used to find if certificate is a CA

AddSubject Used to find if certificate is linked

stateflag devno count

Example

show certchain

ssl-certFile

The following operations can be performed on "ssl-certFile":

rm| import| show|

rm ssl certFile

Deletes the specified certificate file.

Synopsis

rm ssl certFile <name>

Arguments

name Name of the certificate file to delete.

Example

rm ssl certfile my-certfile

import ssl certFile

Imports a certificate file to the Citrix ADC, assigns it a name, and stores it in the /nsconfig/ssl/ certfile folder. The folder is created if it does not exist.

Synopsis

import ssl certFile <name> <src>

Arguments

name Name to assign to the imported certificate file. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

src URL specifying the protocol, host, and path, including file name, to the certificate file to be imported. For example, http://www.example.com/cert_file. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

Example

import ssl certfile my-certfile http://www.example.com/cert_file

show ssl certFile

Displays a list of all the imported certificate file objects on the Citrix ADC.

Synopsis

show ssl certFile

Arguments

Output

name Name to assign to the imported certificate file. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

src URL specifying the protocol, host, and path, including file name, to the certificate file to be imported. For example, http://www.example.com/cert_file. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

devno count stateflag

Example

show ssl certfile

ssl-certKey

The following operations can be performed on "ssl-certKey":

link| set| rm| unlink| bind| clear| unbind| unset| add| show| update|

link ssl certKey

Links a certificate-key pair to its Certificate Authority (CA) certificate-key pair.

Synopsis

link ssl certKey <certkeyName> <linkCertKeyName>

Arguments

certkeyName Name of the certificate-key pair to link to its issuer's certificate-key pair in the chain.

linkCertKeyName Name of the Certificate Authority certificate-key pair to which to link a certificate-key pair.

Example

1)link ssl certkey siteAcertkey CAcertkey In the above example, the certificate-key siteAcertkey is bound to its issuer certificate-key pair CAcertkey.

Related Commands

- show ssl certlink

set ssl certKey

Modifies the specified attributes of a certificate-key pair.

Synopsis

set ssl certKey <certkeyName> [-expiryMonitor (ENABLED | DISABLED)]

Arguments

certkeyName Name of the certificate-key pair to modify.

expiryMonitor Issue an alert when the certificate is about to expire.

Possible values: ENABLED, DISABLED

notificationPeriod Time, in number of days, before certificate expiration, at which to generate an alert that the certificate is about to expire. Minimum value: 10 Maximum value: 100

rm ssl certKey

Removes all the certificate-key pairs, or the specified certificate-key pair, from the appliance. The certificate-key pair is removed only if it is not referenced by any other object. The reference count is updated when the certificate-key pair is bound to an SSL virtual server or linked to another certificate-key pair.

Synopsis

rm ssl certKey <certkeyName> ...

Arguments

certkeyName Name of the certificate-key pair to remove.

deletefromdevice Delete cert/key file from file system.

Example

1)rm ssl certkey siteAcertkey The above command removes the certificate-key pair siteAcertkey from the system. 2) rm certkey siteAcertkey -deletefromdevice The above command removes the certificate-key pair siteAcertkey from the system along with it's cert and key file form file system.

unlink ssl certKey

Unlinks the certificate-key pair from its Certificate-Authority (CA) certificate-key pair.

Synopsis

unlink ssl certKey <certkeyName>

Arguments

certkeyName Name of the certificate-key pair to unlink.

Example

1)unlink ssl certkey siteAcertkey The above example unlinks the certificate 'siteAcertkey' from its Certificate-Authority (CA) certificate.

Related Commands

- show ssl certlink

bind ssl certKey

Binds a certificate-key pair to an SSL virtual server or an SSL service.

Synopsis

bind ssl certKey

Arguments

certkeyName Name of the certificate-key pair.

ocspResponder Name of the OCSP responder to be associated with the CA certificate.

priority Priority of the OCSP responder binding. Minimum value: 1

Example

1)bind ssl certkey cacert -ocspResponder ocsp_ca -priority 1 In the above example, the CA certificate cacert is bound with the OCSP responder ocsp_ca with priority 1, which is highest.

Related Commands

- show ssl vserver

clear ssl certKey

Clear cached ocspStapling response in certkey.

Synopsis

clear ssl certKey <certkeyName> -ocspstaplingCache

Arguments

certkeyName Name for the certificate and private-key pair. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the certificate-key pair is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cert" or 'my cert').

ocspstaplingCache Clear cached ocspStapling response in certkey.

unbind ssl certKey

Unbinds the specified certificate-key pair from the SSL virtual server or service.

Synopsis

unbind ssl certKey <certkeyName> -ocspResponder <string>

Arguments

certkeyName Name of the certificate-key pair to unbind.

ocspResponder Name of the OCSP responder.

Example

1)unbind ssl certkey sslvip siteAcertkey In the above example, the server certificate siteAcertkey is unbound from the SSL virtual server. 2)unbind ssl certkey sslvip CAcertkey -CA In the above example, the CA certificate CAcertkey is unbound from the SSL virtual server.

Related Commands

- show ssl vserver

unset ssl certKey

Use this command to remove ssl certKey settings.Refer to the set ssl certKey command for meanings of the arguments.

Synopsis

unset ssl certKey <certkeyName>

add ssl certKey

Adds a certificate-key pair to memory. After it is bound to a virtual server or service, it is used for processing SSL transactions. In a high-availability configuration, the path to the certificate and the optional private key must be the same on the primary and the secondary appliance. For a server certificate, a private key is required.

Synopsis

add ssl certKey <certkeyName> (-cert <string>) [-expiryMonitor (ENABLED | DISABLED)]

Arguments

certkeyName Name for the certificate and private-key pair. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the certificate-key pair is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cert" or 'my cert').

cert Name of and, optionally, path to the X509 certificate file that is used to form the certificate-key pair. The certificate file should be present on the appliance's hard-disk drive or solid-state drive. Storing a certificate in any location other than the default might cause inconsistency in a high availability setup. /nsconfig/ssl/ is the default path.

key Name of and, optionally, path to the private-key file that is used to form the certificate-key pair. The certificate file should be present on the appliance's hard-disk drive or solid-state drive. Storing a certificate in any location other than the default might cause inconsistency in a high availability setup. /nsconfig/ssl/ is the default path.

password Passphrase that was used to encrypt the private-key. Use this option to load encrypted private-keys in PEM format.

fipsKey Name of the FIPS key that was created inside the Hardware Security Module (HSM) of a FIPS appliance, or a key that was imported into the HSM.

hsmKey Name of the HSM key that was created in the External Hardware Security Module (HSM) of a FIPS appliance.

inform Input format of the certificate and the private-key files. The three formats supported by the appliance are: PEM - Privacy Enhanced Mail DER - Distinguished Encoding Rule PFX - Personal Information Exchange

Possible values: DER, PEM, PFX Default value: PEM

passplain Pass phrase used to encrypt the private-key. Required when adding an encrypted private-key in PEM format.

expiryMonitor Issue an alert when the certificate is about to expire.

Possible values: ENABLED, DISABLED

notificationPeriod Time, in number of days, before certificate expiration, at which to generate an alert that the certificate is about to expire. Minimum value: 10 Maximum value: 100

bundle Parse the certificate chain as a single file after linking the server certificate to its issuer's certificate within the file.

Possible values: YES, NO Default value: NO

Example

1)add ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /nsconfig/ssl/pkey.pem The above command loads a certificate and private key file. 2)add ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /nsconfig/ssl/pkey.pem -password Password: ````` The above command loads a certificate and private key file. Here the private key file is an encrypted key. 3)add ssl certkey fipscert -cert /nsconfig/ssl/cert.pem -fipskey fips1024 The above command loads a certificate and associates it with the corresponding FIPS key that resides within the HSM. 4)add ssl certkey externalhsmcert -cert /nsconfig/ssl/hsmcert.pem -hsmkey key_simple_rsa1 The above command loads a certificate and associates it with the corresponding HSM key that resides within the External HSM.

show ssl certKey

Displays information about all the certificate-key pairs configured on the appliance, or displays detailed information about the specified certificate-key pair.

Synopsis

show ssl certKey

Arguments

certkeyName Name of the certificate-key pair for which to show detailed information.

Output

cert The name and location of the file containing the certificate.

key The name and location of the file containing the key.

inform The encoding format of the certificate and key (PEM,DER or PFX).

signatureAlg Signature algorithm.

CertificateType Specifies whether the certificate is of type root-CA, intermediate-CA, server, client, or client and server

serial Serial number.

issuer Issuer name.

clientCertNotBefore Not-Before date.

clientCertNotAfter Not-After date.

daysToExpiration Days remaining for the certificate to expire.

subject Subject name.

publickey Public key algorithm.

publickeysize Size of the public key.

version Version.

priority ocsp priority

status Status of the certificate.

fipsKey FIPS key ID.

hsmKey External HSM key ID.

passcrypt Passcrypt.

passplain Passplain.

data Vserver Id

serverName Vserver name to which the certificate key pair is bound.

serviceName Service name to which the certificate key pair is bound.

ocspResponder OCSP responders bound to this certkey

sslProfile SSL profile name to which the certificate key pair is bound.

expiryMonitor Certificate expiry monitor

notificationPeriod Certificate expiry notification period

linkCertKeyName The name of the Certificate-Authority.

stateflag sandns Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field. These values are called "Subject Alternative Names" (SAN). This field is for DNS names

sanipadd Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field. These values are called "Subject Alternative Names" (SAN). This field is for IP address

ocspResponseStatus Ocsp response status of the certificate.

ocspBindReferences Number of references to ocspresponder by this certkey

gslbServiceFlag Indicates that this is a gslb service

builtin Flag to determine if Cert key is built-in or not

feature The feature to be checked while applying this config

devno count

Example

1. An example of the output of the show ssl certkey command is shown below: 2 configured certkeys: 1)Name: siteAcertkey Cert Path: /nsconfig/ssl/siteA-cert.pem Key Path: /nsconfig/ssl/siteA-key.pem Format: PEM Status: Valid 2)Name: cert1 Cert Path: /nsconfig/ssl/server_cert.pem Key Path: /nsconfig/ssl/server_key.pem Format: PEM Status: Valid

2. An example of the output of the show ssl certkey siteAcertkey command is shown below: Name: siteAcertkeyStatus: Valid Version: 3 Serial Number: 02 Signature Algorithm: md5WithRSAEncryption Issuer: /C=US/ST=CA/L=Santa Clara/O=siteA/OU=Tech Validity Not Before: Nov 11 14:58:18 2001 GMT Not After: Aug 7 14:58:18 2004 GMT Subject: /C=US/ST-CA/L=San Jose/O=CA/OU=Security Public Key Algorithm: rsaEncryption Public Key size: 1024

update ssl certKey

Updates the certificate or private key in a certificate-key pair. In a high availability configuration, the path to the certificate and the optional private key must be the same on the primary and secondary nodes.

Synopsis

update ssl certKey <certkeyName> [-cert <string>]

Arguments

certkeyName Name of the certificate-key pair to update.

cert Name of and, optionally, path to the X509 certificate file that is used to form the certificate-key pair. The certificate file should be present on the appliance's hard-disk drive or solid-state drive. Storing a certificate in any location other than the default might cause inconsistency in a high availability setup. /nsconfig/ssl/ is the default path.

key Name of and, optionally, path to the private-key file that is used to form the certificate-key pair. The certificate file should be present on the appliance's hard-disk drive or solid-state drive. Storing a certificate in any location other than the default might cause inconsistency in a high availability setup. /nsconfig/ssl/ is the default path.

password Passphrase that was used to encrypt the private-key. Use this option to load encrypted private-keys in PEM format.

fipsKey Name of the FIPS key that was created inside the Hardware Security Module (HSM) of a FIPS appliance, or a key that was imported into the HSM.

inform Input format of the certificate and the private-key files. The three formats supported by the appliance are: PEM - Privacy Enhanced Mail DER - Distinguished Encoding Rule PFX - Personal Information Exchange

Possible values: DER, PEM, PFX Default value: PEM

passplain Pass phrase used to encrypt the private-key. Required when adding an encrypted private-key in PEM format.

noDomainCheck Override the check for matching domain names during a certificate update operation.

Example

1. ```
   update ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /
   nsconfig/ssl/pkey.pem
   ```

The above command updates a certificate and private key file. 2) update ssl certkey siteAcertkey -cert /nsconfig/ssl/cert.pem -key /nsconfig/ssl/pkey.pem -password Password: ```` The above command updates a certificate and private key file. Here the private key file is an encrypted key. 3) update ssl certkey mydomaincert The above command updates the certificate using the same parameters (-cert path/-key path) that it was added with.

Related Commands

- rm ssl certkey

ssl-certKeyBundle

The following operations can be performed on "ssl-certKeyBundle":

show| add| rm|

show ssl certKeyBundle

Displays information about all configured certificate-key bundle's on the appliance, or displays detailed information about the specified certificate-key bundle.

Synopsis

show ssl certKeyBundle

Arguments

certkeyBundleName Name given to the cerKeyBundle. The name will be used to bind/unbind certkey bundle to vip. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC
   ```

CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

Output

bundlefile Name of and, optionally, path to the X509 certificate bundle file that is used to form the certificate-key bundle. The certificate bundle file should be present on the appliance's hard-disk drive or solid-state drive. /nsconfig/ssl/ is the default path. The certificate bundle file consists of list of certificates and one key in PEM format.

passplain Pass phrase used to encrypt the private-key. Required when certificate bundle file contains encrypted private-key in PEM format.

serverName Vserver name to which the certKeyBundle is bound.

subject Subject name.

serial Serial number.

issuer Issuer name.

publickey Public key algorithm.

publickey Public key algorithm.

publickeysize Size of the public key.

sandns Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field. These values are called "Subject Alternative Names" (SAN). This field is for DNS names

sanipadd Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field. These values are called "Subject Alternative Names" (SAN). This field is for IP address

sandns Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field. These values are called "Subject Alternative Names" (SAN). This field is for DNS names

sanipadd Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field. These values are called "Subject Alternative Names" (SAN). This field is for IP address

clientCertNotBefore Not-Before date.

clientCertNotAfter Not-After date.

daysToExpiration Days remaining for the certificate to expire.

signatureAlg Signature algorithm.

status Status of the certificate.

stateflag devno count

Example

1. show ssl certKeyBundle bundle1
2. show ssl certKeyBundle

add ssl certKeyBundle

Adds a certificate-key bundle. After it is bound to a virtual server, it is used for processing SSL transactions.

Synopsis

add ssl certKeyBundle <certkeyBundleName> -bundlefile <input_filename>

Arguments

certkeyBundleName Name given to the cerKeyBundle. The name will be used to bind/unbind certkey bundle to vip. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

bundlefile Name of and, optionally, path to the X509 certificate bundle file that is used to form the certificate-key bundle. The certificate bundle file should be present on the appliance's hard-disk drive or solid-state drive. /nsconfig/ssl/ is the default path. The certificate bundle file consists of list of certificates and one key in PEM format.

passplain Pass phrase used to encrypt the private-key. Required when certificate bundle file contains encrypted private-key in PEM format.

Example

1. add ssl certKeyBundle bundle1 -bundlefile /nsconfig/ssl/cert_bundle.pem

2. add ssl certKeyBundle bundle2 -bundlefile /nsconfig/ssl/cert_bundle_enc.pem -passplain <>

rm ssl certKeyBundle

Removes the specified certificate-key bundle. The certificate-key bundle is removed only if it is not referenced by any SSL virtual server.

Synopsis

rm ssl certKeyBundle <certkeyBundleName>

Arguments

certkeyBundleName Name given to the cerKeyBundle. The name will be used to bind/unbind certkey bundle to vip. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

Example

rm ssl certKeyBundle bundle1

ssl-certLink

The following operations can be performed on "ssl-certLink":

show ssl certLink

Displays information about all the linked certificate-key pairs on the appliance.

Synopsis

show ssl certLink

Arguments

Output

certkeyName Certificate key name.

linkCertKeyName Name of the Certificate-Authority.

devno count stateflag

Example

The following shows an example of the output of the show ssl certlink command: linked certificate:

1. Cert Name: siteAcertkey CA Cert Name: CAcertkey

Related Commands

- unlink ssl certkey

ssl-certReq

The following operations can be performed on "ssl-certReq":

create ssl certReq

Generates a new Certificate Signing Request (CSR). A CSR is a collection of information including the domain name, company details, and the private key to be used to create the certificate. Send the CSR to a Certificate Authority (CA) to obtain an X509 certificate for the user domain (web site).

Synopsis

create ssl certReq <reqFile> (-keyFile <input_filename> | -fipsKeyName <string>) -countryName <string> -stateName <string> -organizationName <string> {-challengePassword }

Arguments

reqFile Name for and, optionally, path to the certificate signing request (CSR). /nsconfig/ssl/ is the default path. Maximum value: 63

keyFile Name of and, optionally, path to the private key used to create the certificate signing request, which then becomes part of the certificate-key pair. The private key can be either an RSA or a DSA key. The key must be present in the appliance's local storage. /nsconfig/ssl is the default path. Maximum value: 63

subjectAltName Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field. These values are called "Subject Alternative Names" (SAN). Names include:

1. Email addresses
2. IP addresses
3. URIs

4. DNS names (this is usually also provided as the Common Name RDN within the Subject field of the main certificate.)
5. Directory names (alternative Distinguished Names to that given in the Subject)

fipsKeyName Name of the FIPS key used to create the certificate signing request. FIPS keys are created inside the Hardware Security Module of the FIPS card.

keyform Format in which the key is stored on the appliance.

Possible values: DER, PEM Default value: PEM

PEMPassPhrase countryName Two letter ISO code for your country. For example, US for United States.

stateName Full name of the state or province where your organization is located. Do not abbreviate.

organizationName Name of the organization that will use this certificate. The organization name (corporation, limited partnership, university, or government agency) must be registered with some authority at the national, state, or city level. Use the legal name under which the organization is registered. Do not abbreviate the organization name and do not use the following characters in the name: Angle brackets (< >) tilde (~), exclamation mark, at (@), pound (#), zero (0), caret (\^), asterisk (*), forward slash (/), square brackets (), question mark (?).

organizationUnitName Name of the division or section in the organization that will use the certificate.

localityName Name of the city or town in which your organization's head office is located.

commonName Fully qualified domain name for the company or web site. The common name must match the name used by DNS servers to do a DNS lookup of your server. Most browsers use this information for authenticating the server's certificate during the SSL handshake. If the server name in the URL does not match the common name as given in the server certificate, the browser terminates the SSL handshake or prompts the user with a warning message. Do not use wildcard characters, such as asterisk (*) or question mark (?), and do not use an IP address as the common name. The common name must not contain the protocol specifier `<http://>` or `<https://>`.

emailAddress Contact person's e-mail address. This address is publically displayed as part of the certificate. Provide an e-mail address that is monitored by an administrator who can be contacted about the certificate.

challengePassword Pass phrase, embedded in the certificate signing request that is shared only between the client or server requesting the certificate and the SSL certificate issuer (typically the certificate authority). This pass phrase can be used to authenticate a client or server that is requesting a certificate from the certificate authority.

companyName Additional name for the company or web site.

digestMethod Digest algorithm used in creating CSR

Possible values: SHA1, SHA256

Example

create ssl certreq /nsconfig/ssl/csr.pem -keyFile /nsconfig/ssl/rsa1024.pem

Related Commands

- create ssl ecdsakey

ssl-certificateChain

The following operations can be performed on "ssl-certificateChain":

show| add|

show ssl certificateChain

Displays information about all the linked certificate-key pairs on the appliance.

Synopsis

show ssl certificateChain

Arguments

certkeyName Name of the certificate-key pair.

Output

chainLinked Certkeys which are currenlty in SSL certificate chain

chainPossibleLinks Certkeys which can be in SSL certificate chain

chainIssuer Name of the issuer

chainComplete Is set to 1 if ssl certificate chain is complete

devno count stateflag

Related Commands

- unlink ssl certkey

add ssl certificateChain

This command is used to form a SSL certificate chain in one shot. For a given CertKey the system will scan all the certificates present in the appliance and then form the appropriate certificate chain automatically.

Synopsis

add ssl certificateChain <certkeyName>

Arguments

certkeyName Name of the certificate-key pair.

ssl-cipher

The following operations can be performed on "ssl-cipher":

add| rm| set| show| unbind| unset| bind|

add ssl cipher

Creates a user-defined cipher group, which you can bind to an SSL virtual server instead of binding ciphers individually. Although you cannot modify a built-in cipher group, you can add built-in cipher groups as well as individual ciphers to a user-defined cipher group.

Synopsis

add ssl cipher <cipherGroupName>

Arguments

cipherGroupName Name for the user-defined cipher group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the cipher group is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my ciphergroup" or 'my ciphergroup').

Example

1. add ssl cipher mygroup SSL2-RC4-MD5 SSL2-EXP-RC4-MD5 The above command creates a new cipher-group by the name: mygroup, with the two ciphers SSL2-RC4-MD5 and SSL2-EXP-RC4-MD5, as part of the cipher-group. If a cipher-group by the name: mygroup already exists in system, then the two ciphers is added to the list of ciphers contained in the group.
2. add ssl cipher mygroup HIGH MEDIUM The above command creates a new cipher-group by the name: mygroup, with the ciphers from the cipher alias "HIGH" and "MEDIUM" as part of the cipher group. If a cipher-group by the name, mygroup, already exists in system, then the ciphers from the two aliases is added to the list of ciphers contained in the group.
3. add ssl cipher cipher_sha The above command creates a new cipher-group by the name: cipher_sha and No ciphers added to the created cipher group.

rm ssl cipher

Removes a user-defined cipher group from the appliance.

Synopsis

rm ssl cipher <cipherGroupName>

Arguments

cipherGroupName Name of the user-defined cipher group to remove.

Example

1)rm ssl cipher mygroup SSL2-RC4-MD5 The above example removes the cipher SSL2-RC4-MD5 from the cipher group mygroup. 2)rm ssl cipher mygroup The above example will remove the cipher group 'mygroup' from the system.

set ssl cipher

Modifies the priority of the cipher within a cipher group.

Synopsis

set ssl cipher <cipherGroupName> (-cipherName <string> -cipherPriority <positive_integer>)

Arguments

cipherGroupName Name of the cipher group.

cipherName Cipher name.

cipherPriority This indicates priority assigned to the particular cipher Minimum value: 1

Example

1. set ssl cipher cipher_sha -cipher TLS1-AES-128-CBC-SHA -cipherpriority 1 The above example sets the priority of TLS1-AES-128-CBC-SHA to 1 within the cipher group cipher_sha.

show ssl cipher

Displays information about all the cipher groups defined on the appliance, or displays detailed information about the specified cipher group.

Synopsis

show ssl cipher

Arguments

cipherGroupName Name of the cipher group for which to show detailed information.

sslProfile Name of the profile to which cipher is attached.

Output

description Cipher suite description.

cipherName Cipher name.

flag stateflag cipherPriority This indicates priority assigned to the particular cipher

peFlags devno count

Example

1. An example of the output of the show ssl cipher SSL3-RC4-MD5 command is as follows: Cipher Name: SSL3-RC4-MD5 Description: SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
2. This example displays the details of individual ciphers in the system predefinedcipher-alias: SSLv3 (the command show ssl cipher SSLv3 has been entered):

3. ```
   Cipher Name: SSL3-RC4-MD5    Priority:1

   Description: SSLv3 Kx=RSA      Au=RSA  Enc=RC4(128)  Mac=MD5
   ```

4. ```
   Cipher Name: SSL3-RC4-SHA    Priority:2

   Description: SSLv3 Kx=RSA      Au=RSA  Enc=RC4(128)  Mac=SHA1
   ```

5. ```
   Cipher Name: SSL3-DES-CBC3-SHA    Priority:3

   Description: SSLv3 Kx=RSA      Au=RSA  Enc=3DES(168) Mac=SHA1
   ```

6. ```
   Cipher Name: SSL3-DES-CBC-SHA    Priority:4

   Description: SSLv3 Kx=RSA      Au=RSA  Enc=DES(56)   Mac=SHA1
   ```

7. ```
   Cipher Name: TLS1-AES-256-CBC-SHA    Priority:5

   Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(256)  Mac=SHA1
   ```

8. ```
   Cipher Name: TLS1-AES-128-CBC-SHA    Priority:6

   Description: SSLv3 Kx=RSA      Au=RSA  Enc=AES(128)  Mac=SHA1
   ```

9. ```
   Cipher Name: SSL3-EXP-RC4-MD5    Priority:7

   Description: SSLv3 Kx=RSA(512) Au=RSA  Enc=RC4(40)   Mac=MD5  Export
   ```

10. ```
    Cipher Name: SSL3-EXP-DES-CBC-SHA    Priority:8

    Description: SSLv3 Kx=RSA(512) Au=RSA  Enc=DES(40)   Mac=SHA1 Export
    ```

11. ```
    Cipher Name: SSL3-EXP-RC2-CBC-MD5    Priority:9

    Description: SSLv3 Kx=RSA(512) Au=RSA  Enc=RC2(40)   Mac=MD5  Export
    ```
    ```

12.
```
Cipher Name: SSL3-EDH-DSS-DES-CBC3-SHA    Priority:10

Description: SSLv3 Kx=DH       Au=DSS  Enc=3DES(168) Mac=SHA1
```

unbind ssl cipher

Removes all the ciphers from a user-defined cipher group. You can only remove individual ciphers from a user-defined cipher group. Removing groups is not supported.

Synopsis

unbind ssl cipher <cipherGroupName>

Arguments

cipherGroupName Name of the user-defined cipher group.

cipherName Name(s) of the cipher(s) to be removed from the user-defined cipher group.

Example

1. rm ssl cipher mygroup SSL2-RC4-MD5 The above example removes the cipher SSL2-RC4-MD5 from the cipher group mygroup.
2. rm ssl cipher mygroup The above example will remove the cipher group 'mygroup' from the system.
3. unbind ssl cipher cipher_sha -cipherName TLS1.2-AES-256-SHA256 The above example will remove the cipher TLS1.2-AES-256-SHA256 from cipher_sha cipher group.

unset ssl cipher

Use this command to remove ssl cipher settings.Refer to the set ssl cipher command for meanings of the arguments.

Synopsis

unset ssl cipher <cipherGroupName> -cipherName -cipherPriority

bind ssl cipher

Adds ciphers to a user-defined cipher group. You can add an existing cipher group to a user-defined cipher group but you cannot modify a built-in cipher group.

Synopsis

bind ssl cipher [<cipherGroupName>@]

Arguments

cipherGroupName Name of the user-defined cipher group.

cipherName Name of the individual cipher, user-defined cipher group, or predefined (built-in) cipher alias to add to the cipher group.

cipherPriority Priority of the cipher to be added Minimum value: 1 Maximum value: 1000

Example

1. bind ssl cipher sslvip ADD SSL3-RC4-SHA The above example appends the cipher SSL3-RC4-SHA to the cipher-suite already configured for the SSL virtual server sslvip.
2. bind ssl cipher sslvip REM NULL The above example removes the ciphers identified by the system's predefined cipher-alias -NULL from the cipher-suite already configured for the SSL virtual server sslvip.
3. bind ssl cipher sslvip ORD HIGH The above example overrides the existing cipher-suite configured for the SSL virtual server with ciphers, having HIGH encryption strength (ciphers supporting 168-bit encryption).
4. bind ssl cipher cipher_sha -cipherName TLS1.2-AES-128-SHA256 The above example adds the cipher TLS1.2-AES-128-SHA256 to the cipher group cipher_sha. Priority of added cipersuite will be next available maximum value in cipher group cipher_sha. 3i) bind ssl cipher cipher_sha -cipherName TLS1.2-AES-128-SHA256 -cipherPriority 5 The above example adds the cipher TLS1.2-AES-128-SHA256 to the cipher group cipher_sha at priority 5. If cipher already bounded at higher priority in the cipher group, then cipher priority remains same.

Note: The individual ciphers contained in a system predefined cipher-alias can beviewed by using the following command: show ssl cipher <cipherAlaisName>

Related Commands

- show ssl vserver

ssl-ciphersuite

The following operations can be performed on "ssl-ciphersuite":

show ssl ciphersuite

Displays information about all the cipher suites configured on the appliance, or displays detailed information about the specified cipher-suite. A cipher suite comprises a protocol and the following algorithms: key exchange (Kx), authentication (Au), encryption (Enc), and message authentication code (Mac).

Synopsis

show ssl ciphersuite

Arguments

cipherName Name of the cipher suite for which to show detailed information.

Output

description Cipher suite description.

flag stateflag devno count

Example

1. An example of the output of the show ssl cipher SSL3-RC4-MD5 command is as follows: Cipher Name: SSL3-RC4-MD5 Description: SSLv3 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
2. This example displays the details of individual ciphers in the system predefinedcipher-alias: SSLv2 (the command show ssl cipher SSLv2 has been entered): 8 configured cipher(s)in alias
3. Cipher Name: SSL2-RC4-MD5 Description: SSLv2 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5
4. Cipher Name: SSL2-EXP-RC4-MD5 Description: SSLv2 Kx=RSA(512) Au=RSA Enc=RC4(40) Mac=MD5 export
5. Cipher Name: SSL2-RC2-CBC-MD5 Description: SSLv2 Kx=RSA Au=RSA Enc=RC2(128) Mac=MD5
6. Cipher Name: SSL2-EXP-RC2-CBC-MD5 Description: SSLv2 Kx=RSA(512) Au=RSA Enc=RC2(40) Mac=MD5 export
7. Cipher Name: SSL2-DES-CBC-MD5 Description: SSLv2 Kx=RSA Au=RSA Enc=DES(56) Mac=MD5
8. Cipher Name: SSL2-DES-CBC3-MD5 Description: SSLv2 Kx=RSA Au=RSA Enc=3DES(168) Mac=MD5

9. Cipher Name: SSL2-RC4-64-MD5 Description: SSLv2 Kx=RSA Au=RSA Enc=RC4(64) Mac=MD5

Ssl

The entities on which you can perform NetScaler CLI operations:

- ssl-action
- ssl-caCertGroup
- ssl-cert
- ssl-certBundle
- ssl-certChain
- ssl-certFile
- ssl-certKey
- ssl-certKeyBundle
- ssl-certLink
- ssl-certReq
- ssl-certificateChain
- ssl-cipher
- ssl-ciphersuite
- ssl-crl
- ssl-crlFile
- ssl-dhFile
- ssl-dhParam
- ssl-dtlsProfile
- ssl-ecdsaKey
- ssl-fips
- ssl-fipsKey
- ssl-fipsSIMSource
- ssl-fipsSIMTarget
- ssl-global
- ssl-hsmKey

- ssl-keyFile
- ssl-logprofile
- ssl-ocspResponder
- ssl-parameter
- ssl-pkcs12
- ssl-pkcs8
- ssl-policy
- ssl-policylabel
- ssl-profile
- ssl-rsakey
- ssl-service
- ssl-serviceGroup
- ssl
- ssl-stats
- ssl-vserver
- ssl-wrapkey

ssl-crl

The following operations can be performed on "ssl-crl":

rm| add| unset| set| show| create|

rm ssl crl

Removes the specified CRL from the appliance.

Synopsis

rm ssl crl <crlName> ...

Arguments

crlName Name of the CRL to remove.

Example

1)rm ssl crl ca_crl The above CLI command to delete the CRL object ca_crl from the system is.

add ssl crl

Adds a Certificate Revocation List (CRL). A CRL identifies invalid certificates by serial number and issuer. In a high availability configuration, the CRL must be in the same location on the primary and secondary nodes.

Synopsis

add ssl crl <crlName> <crlPath> {-password }

Arguments

crlName Name for the Certificate Revocation List (CRL). Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the CRL is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my crl" or 'my crl').

crlPath Path to the CRL file. /var/netscaler/ssl/ is the default path.

inform Input format of the CRL file. The two formats supported on the appliance are: PEM - Privacy Enhanced Mail. DER - Distinguished Encoding Rule.

Possible values: DER, PEM Default value: PEM

refresh Set CRL auto refresh.

Possible values: ENABLED, DISABLED

CAcert CA certificate that has issued the CRL. Required if CRL Auto Refresh is selected. Install the CA certificate on the appliance before adding the CRL.

method Method for CRL refresh. If LDAP is selected, specify the method, CA certificate, base DN, port, and LDAP server name. If HTTP is selected, specify the CA certificate, method, URL, and port. Cannot be changed after a CRL is added.

Possible values: HTTP, LDAP

server IP address of the LDAP server from which to fetch the CRLs.

url URL of the CRL distribution point.

port Port for the LDAP server. Minimum value: 1

baseDN Base distinguished name (DN), which is used in an LDAP search to search for a CRL. Citrix recommends searching for the Base DN instead of the Issuer Name from the CA certificate, because the Issuer Name field might not exactly match the LDAP directory structure's DN.

scope Extent of the search operation on the LDAP server. Available settings function as follows: One - One level below Base DN. Base - Exactly the same level as Base DN.

Possible values: Base, One Default value: One

interval CRL refresh interval. Use the NONE setting to unset this parameter.

Possible values: MONTHLY, WEEKLY, DAILY, NOW, NONE

day Day on which to refresh the CRL, or, if the Interval parameter is not set, the number of days after which to refresh the CRL. If Interval is set to MONTHLY, specify the date. If Interval is set to WEEKLY, specify the day of the week (for example, Sun=0 and Sat=6). This parameter is not applicable if the Interval is set to DAILY. Minimum value: 0 Maximum value: 31

time Time, in hours (1-24) and minutes (1-60), at which to refresh the CRL.

bindDN Bind distinguished name (DN) to be used to access the CRL object in the LDAP repository if access to the LDAP repository is restricted or anonymous access is not allowed.

password Password to access the CRL in the LDAP repository if access to the LDAP repository is restricted or anonymous access is not allowed.

binary Set the LDAP-based CRL retrieval mode to binary.

Possible values: YES, NO Default value: NO

Example

1)add ssl certkey CAcert -cert /nsconfig/ssl/ca_cert.pem add ssl crl crl_file /var/netscaler/ssl/crl.pem -cacert CAcert The above command adds a CRL from local storage system (HDD) with no refresh set. 2)add ssl certkey CAcert -cert /nsconfig/ssl/ca_cert.pem add ssl crl crl_file /var/netscaler/ssl/crl_new.pem -cacert Cacert -refresh ENABLED -server 10.102.1.100 -port 389 -interval DAILY -baseDN o=example.com,ou=security,c=US The above command adds a CRL to the system by fetching the CRL from the LDAP server and setting the refresh interval as daily.

unset ssl crl

Use this command to remove ssl crl settings.Refer to the set ssl crl command for meanings of the arguments.

Synopsis

unset ssl crl <crlName>

set ssl crl

Modifies all the parameters of a CRL, except the CRL name and method.

Synopsis

set ssl crl <crlName> {-password }

Arguments

crlName Name of the CRL to be modified.

refresh Set CRL auto refresh.

Possible values: ENABLED, DISABLED

CAcert CA certificate that has issued the CRL. Required if CRL Auto Refresh is selected. Install the CA certificate on the appliance before adding the CRL.

server IP address of the LDAP server from which to fetch the CRLs.

method Method for CRL refresh. If LDAP is selected, specify the method, CA certificate, base DN, port, and LDAP server name. If HTTP is selected, specify the CA certificate, method, URL, and port. Cannot be changed after a CRL is added.

Possible values: HTTP, LDAP

url URL of the CRL distribution point.

port Port for the LDAP server. Minimum value: 1

baseDN Base distinguished name (DN), which is used in an LDAP search to search for a CRL. Citrix recommends searching for the Base DN instead of the Issuer Name from the CA certificate, because the Issuer Name field might not exactly match the LDAP directory structure's DN.

scope Extent of the search operation on the LDAP server. Available settings function as follows: One - One level below Base DN. Base - Exactly the same level as Base DN.

Possible values: Base, One Default value: One

interval CRL refresh interval. Use the NONE setting to unset this parameter.

Possible values: MONTHLY, WEEKLY, DAILY, NOW, NONE

day Day on which to refresh the CRL, or, if the Interval parameter is not set, the number of days after which to refresh the CRL. If Interval is set to MONTHLY, specify the date. If Interval is set to WEEKLY, specify the day of the week (for example, Sun=0 and Sat=6). This parameter is not applicable if the Interval is set to DAILY. Minimum value: 0 Maximum value: 31

time Time, in hours (1-24) and minutes (1-60), at which to refresh the CRL.

bindDN Bind distinguished name (DN) to be used to access the CRL object in the LDAP repository if access to the LDAP repository is restricted or anonymous access is not allowed.

password Password to access the CRL in the LDAP repository if access to the LDAP repository is restricted or anonymous access is not allowed.

binary Set the LDAP-based CRL retrieval mode to binary.

Possible values: YES, NO Default value: NO

Example

1)set ssl crl crl_file -refresh ENABLE -interval MONTHLY -days 10 -time 12:00 The above example sets the CRL refresh to every Month, on date=10, and time=12:00hrs. 2)set ssl crl crl_file -refresh ENABLE -interval WEEKLY -days 1 -time 00:10 The above example sets the CRL refresh every Week, on weekday=Monday, and at time 10 past midnight. 3)set ssl crl crl_file -refresh ENABLE -interval DAILY -days 1 -time 12:00 The above example sets the CRL refresh every Day, at 12:00hrs. 4)set ssl crl crl_file -refresh ENABLE -days 10 The above example sets the CRL refresh after every 10 days. Note: The CRL will be refreshed after every 10 days. The time for CRL refresh will be 00:00 hrs. 5)set ssl crl crl_file -refresh ENABLE -time 01:00 The above example sets the CRL refresh after every 1 hour. 6)set ssl crl crl_file -refresh ENABLE -interval NOW The above example sets the CRL refresh instantaneously.

show ssl crl

Displays information about all the CRLs configured on the appliance, or displays detailed information about the specified CRL.

Synopsis

show ssl crl

Arguments

crlName Name of the CRL for which to show detailed information.

Output

crlPath The name and path to the file containing the CRL.

inform The encoding format of the CRL (PEM or DER).

CAcert The CA certificate that issued the CRL.

refresh The state of the auto refresh feature for the CRL.

scope Extent of the search operation on the LDAP server. Base: Exactly the same level as basedn One : One level below basedn.

server The IP address of the LDAP/HTTP server from which the CRLs are to be fetched.

port The port of the LDAP/HTTP server.

url URL of the CRL distribution point.

method The method for CRL refresh (LDAP or HTTP).

baseDN The baseDN to be used to fetch the CRL object from the LDAP server.

interval The CRL refresh interval.

day The day when the CRL is to be refreshed.

time The time when the CRL is to be refreshed.

bindDN The bindDN to be used to access the CRL object in the LDAP repository.

password The password to be is used to access the CRL object in the LDAP repository.

flags CRL status flag.

lastupdatetime Last CRL refresh time.

version CRL version.

signaturealgo Signature algorithm.

issuer Issuer name.

lastupdate Last update time.

nextupdate Next update time.

date Certificate Revocation date

number Certificate Serial number.

binary Mode of retrieval of CRL from LDAP server.

daysToExpiration Number of days remaining for the CRL to expire.

devno count stateflag

Example

1. An example output of the show ssl crl command is as follows: 1 configured CRL(s) 1 Name: ca_crl CRL Path: /var/netscaler/ssl/cr1.der Format: DER Cacert: ca_cert Refresh: DISABLED
2. An example of the output of the show ssl crl ca_crl command is as follows: Name: ca_crl Status: Valid, Days to expiration: 21 CRL Path: /var/netscaler/ssl/cr1.der Format: DERCAcert: ca_cert Refresh: DISABLED Version: 1 Signature Algorithm: md5WithRSAEncryption Issuer: /C=US/ST=CA/L=santa clara /O=CA/OU=security Last_update:Dec 21 09:47:16 2001 GMT Next_update:Jan 20 09:47:16 2002 GMT Revoked Certificates: Serial Number: 01 Revocation Date:Dec 21 09:47:02 2001 GMT Serial Number: 02 Revocation Date:Dec 21 09:47:02 2001 GMT

create ssl crl

Revokes a certificate, or list of certificates, or generates a CRL for the list of revoked certificates.

Synopsis

create ssl crl <CAcertFile> <CAkeyFile> <indexFile> (-revoke <input_filename> | -genCRL <output_filename>) {-password }

Arguments

CAcertFile Name of and, optionally, path to the CA certificate file. /nsconfig/ssl/ is the default path. Maximum value: 63

CAkeyFile Name of and, optionally, path to the CA key file. /nsconfig/ssl/ is the default path Maximum value: 63

indexFile Name of and, optionally, path to the file containing the serial numbers of all the certificates that are revoked. Revoked certificates are appended to the file. /nsconfig/ssl/ is the default path Maximum value: 63

revoke Name of and, optionally, path to the certificate to be revoked. /nsconfig/ssl/ is the default path. Maximum value: 63

genCRL Name of and, optionally, path to the CRL file to be generated. The list of certificates that have been revoked is obtained from the index file. /nsconfig/ssl/ is the default path. Maximum value: 63

password Password for the CA key file. Maximum value: 31

Example

1)create crl /nsconfig/ssl/cacert.pem /nsconfig/ssl/cakey.pem /nsconfig/ssl/index.txt -gencrl /var/netscaler/ssl/crl.pem

ssl-crlFile

The following operations can be performed on "ssl-crlFile":

show| rm| import|

show ssl crlFile

Displays a list of all the imported CRL file objects on the Citrix ADC.

Synopsis

show ssl crlFile

Arguments

Output

name Name to assign to the imported CRL file. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

src URL specifying the protocol, host, and path, including file name to the CRL file to be imported. For example, http://www.example.com/crl_file. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

devno count stateflag

Example

show ssl crlfile

rm ssl crlFile

Deletes the specified CRL file.

Synopsis

rm ssl crlFile <name>

Arguments

name Name of the CRL file to delete.

Example

rm ssl crlfile my-crlfile

import ssl crlFile

Imports a CRL file to the Citrix ADC, assigns it a name, and stores it in the /var/netscaler/ssl/crlfile folder. The folder is created if it does not exist.

Synopsis

import ssl crlFile <name> <src>

Arguments

name Name to assign to the imported CRL file. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

src URL specifying the protocol, host, and path, including file name to the CRL file to be imported. For example, http://www.example.com/crl_file. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

Example

import ssl crlfile my-crlfile http://www.example.com/crl_file

ssl-dhFile

The following operations can be performed on "ssl-dhFile":

show| import| rm|

show ssl dhFile

Displays a list of all the imported DH file objects on the Citrix ADC.

Synopsis

show ssl dhFile

Arguments

Output

name Name to assign to the imported DH file. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

src URL specifying the protocol, host, and path, including file name, to the DH file to be imported. For example, http://www.example.com/dh_file. NOTE: The import fails if the file is on an HTTPS server that requires client certificate authentication for access.

devno count stateflag

Example

show ssl dhfile

import ssl dhFile

Imports a DH file to the Citrix ADC, assigns it a name, and stores it in the /nsconfig/ssl/dhfile folder. The folder is created if it does not exist.

Synopsis

import ssl dhFile <name> <src>

Arguments

name Name to assign to the imported DH file. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

src URL specifying the protocol, host, and path, including file name, to the DH file to be imported. For example, http://www.example.com/dh_file. NOTE: The import fails if the file is on an HTTPS server that requires client certificate authentication for access.

Example

import ssl dhfile my-dhfile http://www.example.com/dh_file

rm ssl dhFile

Deletes the specified DH file.

Synopsis

rm ssl dhFile <name>

Arguments

name Name of the DH file to delete.

Example

rm ssl dhfile my-dhfile

ssl-dhParam

The following operations can be performed on "ssl-dhParam":

create ssl dhParam

Generates a Diffie-Hellman (DH) key.

Synopsis

create ssl dhParam <dhFile>

Arguments

dhFile Name of and, optionally, path to the DH key file. /nsconfig/ssl/ is the default path. Maximum value: 63

bits Size, in bits, of the DH key being generated. Minimum value: 512 Maximum value: 2048

gen Random number required for generating the DH key. Required as part of the DH key generation algorithm.

Possible values: 2, 5 Default value: 2

Example

1)create ssl dhparam /nsconfig/ssl/dh1024.pem 1024 -gen 5

Related Commands

- show ssl vserver

ssl-dtlsProfile

The following operations can be performed on "ssl-dtlsProfile":

set| add| rm| show| unset|

set ssl dtlsProfile

Set/modify DTLS profile values

Synopsis

set ssl dtlsProfile <name>

Arguments

name Name for the DTLS profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),equals sign (=), and hyphen (-) characters. Cannot be changed after the profile is created.

pmtuDiscovery Source for the maximum record size value. If ENABLED, the value is taken from the PMTU table. If DISABLED, the value is taken from the profile.

Possible values: ENABLED, DISABLED Default value: DISABLED

maxRecordSize Maximum size of records that can be sent if PMTU is disabled. Default value: 1459 Minimum value: 250 Maximum value: 1459

maxRetryTime Wait for the specified time, in seconds, before resending the request. Default value: 3 Minimum value: 0

helloVerifyRequest Send a Hello Verify request to validate the client.

Possible values: ENABLED, DISABLED Default value: ENABLED

terminateSession Terminate the session if the message authentication code (MAC) of the client and server do not match.

Possible values: ENABLED, DISABLED Default value: DISABLED

maxPacketSize Maximum number of packets to reassemble. This value helps protect against a fragmented packet attack. Default value: 120 Minimum value: 0 Maximum value: 86400

maxHoldQLen Maximum number of datagrams that can be queued at DTLS layer for processing Default value: 32 Minimum value: 32 Maximum value: 65535

maxBadmacIgnorecount Maximum number of bad MAC errors to ignore for a connection prior disconnect. Disabling parameter terminateSession terminates session immediately when bad MAC is detected in the connection. Default value: 100 Minimum value: 1 Maximum value: 65535

Example

set dtlsprofile <profile name> -dropInvalReqs ON -markHttp09Inval ON

add ssl dtlsProfile

Create a new DTLS profile on the Citrix ADC.

Synopsis

add ssl dtlsProfile <name>

Arguments

name Name for the DTLS profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),equals sign (=), and hyphen (-) characters. Cannot be changed after the profile is created.

pmtuDiscovery Source for the maximum record size value. If ENABLED, the value is taken from the PMTU table. If DISABLED, the value is taken from the profile.

Possible values: ENABLED, DISABLED Default value: DISABLED

maxRecordSize Maximum size of records that can be sent if PMTU is disabled. Default value: 1459 Minimum value: 250 Maximum value: 1459

maxRetryTime Wait for the specified time, in seconds, before resending the request. Default value: 3 Minimum value: 0

helloVerifyRequest Send a Hello Verify request to validate the client.

Possible values: ENABLED, DISABLED Default value: ENABLED

terminateSession Terminate the session if the message authentication code (MAC) of the client and server do not match.

Possible values: ENABLED, DISABLED Default value: DISABLED

maxPacketSize Maximum number of packets to reassemble. This value helps protect against a fragmented packet attack. Default value: 120 Minimum value: 0 Maximum value: 86400

maxHoldQLen Maximum number of datagrams that can be queued at DTLS layer for processing Default value: 32 Minimum value: 32 Maximum value: 65535

maxBadmacIgnorecount Maximum number of bad MAC errors to ignore for a connection prior disconnect. Disabling parameter terminateSession terminates session immediately when bad MAC is detected in the connection. Default value: 100 Minimum value: 1 Maximum value: 65535

Example

add dtlsProfile dtls1 -helloVerifyRequest ENABLED -maxRetryTime 4

rm ssl dtlsProfile

Remove a DTLS profile on the Citrix ADC

Synopsis

rm ssl dtlsProfile <name>

Arguments

name Name of the DTLS profile

Example

rm dtlsprofile <profile name>

show ssl dtlsProfile

Display all the configured DTLS profiles in the system. If a name is specified, then only that profile is shown.

Synopsis

show ssl dtlsProfile

Arguments

name Name of the DTLS profile.

Output

pmtuDiscovery PMTU Discovery

maxRecordSize Maximum record size

maxRetryTime Maximum retry time

helloVerifyRequest Hello Verify Request

terminateSession Terminate Session

maxPacketSize Maximum Packet Size

maxHoldQLen Maximum number of datagrams that can be queued at DTLS layer for processing

maxBadmacIgnorecount Maximum number of bad MAC errors to ignore for a connection prior disconnect. Disabling parameter terminateSession terminates session immediately when bad MAC is detected in the connection.

builtin Flag to determine whether dtls profile is built-in or not

feature The feature to be checked while applying this config

devno count stateflag

Example

show dtls profile

unset ssl dtlsProfile

Use this command to remove ssl dtlsProfile settings.Refer to the set ssl dtlsProfile command for meanings of the arguments.

Synopsis

unset ssl dtlsProfile <name>

ssl-ecdsaKey

The following operations can be performed on "ssl-ecdsaKey":

create ssl ecdsaKey

Generates an ECDSA key.

Synopsis

create ssl ecdsaKey <keyFile> -curve (P_256 | P_384) {-password }

Arguments

keyFile Name for and, optionally, path to the ECDSA key file. /nsconfig/ssl/ is the default path. Maximum value: 63

curve Curve id to generate ECDSA key. Only P_256 and P_384 are supported

Possible values: P_256, P_384 Default value: FIPSEXP_F4

keyform Format in which the ECDSA key file is stored on the appliance.

Possible values: DER, PEM Default value: PEM

des Encrypt the generated ECDSA key by using the DES algorithm. On the command line, you are prompted to enter the pass phrase (password) that is used to encrypt the key.

des3 Encrypt the generated ECDSA key by using the Triple-DES algorithm. On the command line, you are prompted to enter the pass phrase (password) that is used to encrypt the key.

aes256 Encrypt the generated ECDSA key by using the AES algorithm.

password Pass phrase to use for encryption if DES or DES3 option is selected. Maximum value: 31

pkcs8 Create the private key in PKCS#8 format.

Example

create ssl ecdsakey /nsconfig/ssl/ecdsa256.key 1024 -curve P_256

Related Commands

- add ssl certkey

ssl-fips

The following operations can be performed on "ssl-fips":

set| unset| show| reset| update|

set ssl fips

Initializes the Hardware Security Module (HSM) on the FIPS card and sets a new security officer password and user password. CAUTION: This command erases all data on the FIPS card. You are prompted before proceeding with the command execution. A restart is required before and after executing this command for the changes to apply. Save the configuration after executing this command and before restarting the appliance.

Synopsis

set ssl fips -initHSM Level-2

Arguments

initHSM FIPS initialization level. The appliance currently supports Level-2 (FIPS 140-2).

Possible values: Level-2

soPassword Security officer password that will be in effect after you have configured the HSM.

oldSoPassword Old password for the security officer.

userPassword The Hardware Security Module's (HSM) User password.

hsmLabel Label to identify the Hardware Security Module (HSM).

Example

1. set fips -initHSM Level-2 fipsso123 oldfipsso123 fipuser123 -hsmLabel FIPS-140-2

> This command will erase all data on the FIPS card. You must save the configuration (saveconfig) after executing this command.Do you want to continue?(Y/N)y

> The above command initializes the FIPS card to FIPS-140-2 Level-2 and sets the HSM's Security Officer and User passwords.

unset ssl fips

Use this command to remove ssl fips settings.Refer to the set ssl fips command for meanings of the arguments.

Synopsis

unset ssl fips -hsmLabel

show ssl fips

Displays the information on the FIPS card.

Synopsis

show ssl fips

Arguments

Output

initHSM The level of the FIPS initialization.

soPassword Security officer password that will be in effect after you have configured the HSM.

userPassword The Hardware Security Module's (HSM) User password.

oldSoPassword Old password for the security officer.

eraseData Erase data.

hsmLabel FIPS card (HSM) label

serial FIPS card serial number.

majorVersion Firmware major version.

minorVersion Firmware minor version.

FipsHwMajorVersion FIPS card hardware major version.

FipsHwMinorVersion FIPS card hardware minor version.

FipsHwVersionString FIPS card hardware extended version string.

flashMemoryTotal Total size of the flash memory on card.

flashMemoryFree Total size of free flash memory.

sramTotal Total size of the SRAM memory on card.

sramFree Total size of free SRAM memory.

status Status.

flag Internal Flags.

serialNo FIPS card serial number.

model FIPS card model info.

state FIPS card state.

firmwareReleaseDate FIPS card firmware revision date.

coresMax Maximum number of crypto cores present in the FIPS card.

coresEnabled Number of crypto cores enabled in the FIPS card.

Example

An example of the output for show ssl fips command is as follows: FIPS HSM Info: HSM Label : FIPS1 Initialization : FIPS-140-2 Level-2 HSM Serial Number : 238180016 Firmware Version : 4.3.0 Total Flash Memory : 1900428 Free Flash Memory : 1899720 Total SRAM Memory : 26210216 Free SRAM Memory : 17857232

reset ssl fips

Resets the FIPS card to the default password for Security Officer and User accounts. This command can be used only if the FIPS card has been locked because of three or more unsuccessful login attempts.

Synopsis

reset ssl fips

Arguments

Example

reset fips

update ssl fips

Updates the FIPS firmware. Note: Upgrade with compatible firmware is required. You must specify a valid file path and name

Synopsis

update ssl fips -fipsFW <string>

Arguments

fipsFW Path to the FIPS firmware file.

Example

update ssl fips -fipsFW /var/nsinstall/fips/CN16XX-NFBE-FW-2.2-130001

ssl-fipsKey

The following operations can be performed on "ssl-fipsKey":

export| show| create| rm| import|

export ssl fipsKey

Exports a FIPS key from one appliance to another or backs up a FIPS key in a secure manner. The exported key is secured by using a strong asymmetric key encryption method.

Synopsis

export ssl fipsKey <fipsKeyName> -key <string>

Arguments

fipsKeyName Name of the FIPS key to export.

key Name of and, optionally, path to the exported key file. /nsconfig/ssl/ is the default path.

Example

export fipskey fips1 -key /nsconfig/ssl/fips1.key

show ssl fipsKey

Displays information about all the FIPS keys configured on the appliance, or displays detailed information about the specified FIPS key.

Synopsis

show ssl fipsKey

Arguments

fipsKeyName Name of the FIPS key for which to show detailed information.

Output

modulus The modulus of the RSA key.

exponent The exponent value for the RSA key.

curve The curve id for the ECDSA key.

keytype The type for the key.

size Size.

devno count stateflag

Example

1. An example of output of show ssl fipskey command is as follows: show fipskey 2 FIPS keys:
2. ```
   FIPS Key Name: fips1
   ```
3. ```
   FIPS Key Name: fips2
   ```
4. An example of output of show fipskey command with FIPS key name specified is as follows: show fipskey fips1 FIPS Key Name: fips1 Modulus: 1024 Public Exponent: 3 (Hex: 0x3)

create ssl fipsKey

Generates a FIPS key within the Hardware Security Module (HSM) of the FIPS card.

Synopsis

create ssl fipsKey <fipsKeyName> -keytype (RSA | ECDSA)

Arguments

fipsKeyName Name for the FIPS key. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the FIPS key is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my fipskey" or 'my fipskey').

keytype Only RSA key and ECDSA Key are supported.

Possible values: RSA, ECDSA Default value: RSA

exponent Exponent value for the FIPS key to be created. Available values function as follows: 3=3 (hexadecimal) F4=10001 (hexadecimal)

Possible values: 3, F4 Default value: 3

modulus Modulus, in multiples of 64, of the FIPS key to be created. Minimum value: 0 Maximum value: 4096

curve Only p_256 (prime256v1) and P_384 (secp384r1) are supported.

Possible values: P_256, P_384 Default value: P_256

Example

create fipskey fips1 -modulus 1024 -exp f4

rm ssl fipsKey

Removes all the FIPS keys, or the specified FIPS key, from the appliance.

Synopsis

rm ssl fipsKey <fipsKeyName> ...

Arguments

fipsKeyName Name of the FIPS key to remove.

Example

rm fipskey fips1

import ssl fipsKey

Imports a FIPS key into the Hardware Security Module (HSM) of the FIPS card. Can import an existing FIPS key, or can import, as a FIPS key, an external private key, such as a key that was created on an Apache or IIS external Web server.

Synopsis

import ssl fipsKey <fipsKeyName> -key <string>

Arguments

fipsKeyName Name for the FIPS key to be imported. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the FIPS key is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my fipskey" or 'my fipskey').

key Name of and, optionally, path to the key file to be imported. /nsconfig/ssl/ is the default path.

inform Input format of the key file. Available formats are: SIM - Secure Information Management; select when importing a FIPS key. If the external FIPS key is encrypted, first decrypt it, and then import it. PEM - Privacy Enhanced Mail; select when importing a non-FIPS key.

Possible values: SIM, DER, PEM Default value: SIM

wrapKeyName Name of the wrap key to use for importing the key. Required for importing a non-FIPS key.

iv Initialization Vector (IV) to use for importing the key. Required for importing a non-FIPS key.

exponent Exponent value for the FIPS key to be created. Available values function as follows: 3=3 (hexadecimal) F4=10001 (hexadecimal)

Possible values: 3, F4 Default value: 3

Example

1)import fipskey fips1 -key /nsconfig/ssl/fipskey.sim The above example imports a FIPS key stored in the file fipskey.sim in the system. 2)import fipskey fips2 -key /nsconfig/ssl/key.der -inform DER -wrapKeyName wrapkey1 -iv wrap123 The above example imports a non-FIPS key stored in the file key.der in the system.

ssl-fipsSIMSource

The following operations can be performed on "ssl-fipsSIMSource":

enable| init|

enable ssl fipsSIMSource

Enable the source FIPS appliance to participate in a secure exchange of keys with the target (secondary) FIPS appliance.

Synopsis

enable ssl fipsSIMSource <targetSecret> <sourceSecret>

Arguments

targetSecret Name of and, optionally, path to the target FIPS appliance's secret data. /nsconfig/ssl/ is the default path.

sourceSecret Name for and, optionally, path to the source FIPS appliance's secret data. /nsconfig/ssl/ is the default path.

Example

enable fipsSIMsource /nsconfig/ssl/target.secret /nsconfig/ssl/source.secret

init ssl fipsSIMSource

Initialize the source FIPS appliance for participating in a secure exchange of keys with the target (secondary) FIPS appliance.

Synopsis

init ssl fipsSIMSource <certFile>

Arguments

certFile Name for and, optionally, path to the source FIPS appliance's certificate file. /nsconfig/ssl/ is the default path.

Example

init fipsSIMsource /nsconfig/ssl/source.cert

ssl-fipsSIMTarget

The following operations can be performed on "ssl-fipsSIMTarget":

enable| init|

enable ssl fipsSIMTarget

Enables secure transfer of FIPS keys in a high availability setup from the primary appliance to the secondary appliance.

Synopsis

enable ssl fipsSIMTarget <keyVector> <sourceSecret>

Arguments

keyVector Name of and, optionally, path to the target FIPS appliance's key vector. /nsconfig/ssl/ is the default path.

sourceSecret Name of and, optionally, path to the source FIPS appliance's secret data. /nsconfig/ssl/ is the default path.

Example

enable fipsSIMtarget /nsconfig/ssl/target.key /nsconfig/ssl/source.secret

init ssl fipsSIMTarget

Initialize the target (secondary) FIPS appliance for participating in a secure exchange of keys with the primary FIPS appliance.

Synopsis

init ssl fipsSIMTarget <certFile> <keyVector> <targetSecret>

Arguments

certFile Name of and, optionally, path to the source FIPS appliance's certificate file. /nsconfig/ssl/ is the default path.

keyVector Name for and, optionally, path to the target FIPS appliance's key vector. /nsconfig/ssl/ is the default path.

targetSecret Name for and, optionally, path to the target FIPS appliance's secret data. The default input path for the secret data is /nsconfig/ssl/.

Example

init fipsSIMtarget /nsconfig/ssl/source.cert /nsconfig/ssl/target.key /nsconfig/ssl/target.secret

ssl-global

The following operations can be performed on "ssl-global":

bind| show| unbind|

bind ssl global

Binds an SSL policy globally.

Synopsis

bind ssl global

Arguments

policyName Name of the SSL policy.

priority Integer specifying the policy's priority. The lower the number, the higher the priority. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.

- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label. Default value: "END"

type Global bind point to which to bind the policy. If CONTROL_OVERRIDE or DATA_OVERRIDE is selected, the global control or data policy overrides the control or data policy bound to the virtual server or service.

Possible values: CONTROL_OVERRIDE, CONTROL_DEFAULT, DATA_OVERRIDE, DATA_DEFAULT, HTTPQUIC_CONTROL_OVERRIDE, HTTPQUIC_CONTROL_DEFAULT, HTTPQUIC_DATA_OVERRIDE, HTTPQUIC_DATA_DEFAULT

invoke Invoke policies bound to a virtual server, service, or policy label. After the invoked policies are evaluated, the flow returns to the policy with the next priority.

labelType Type of policy label to invoke. Specify virtual server for a policy label associated with a virtual server, or policy label for a user-defined policy label.

Possible values: vserver, service, policylabel

labelName Name of the virtual server or user-defined policy label to invoke if the policy evaluates to TRUE.

Example

bind ssl global -policyName certInsert_pol -priority 100

show ssl global

Displays globally bound SSL policies.

Synopsis

show ssl global

Arguments

type Global bind point to which the policy is bound.

Possible values: CONTROL_OVERRIDE, CONTROL_DEFAULT, DATA_OVERRIDE, DATA_DEFAULT, HTTPQUIC_CONTROL_OVERRIDE, HTTPQUIC_CONTROL_DEFAULT, HTTPQUIC_DATA_OVERRIDE, HTTPQUIC_DATA_DEFAULT

Output

stateflag policyName The name for the SSL policy.

priority The priority of the policy binding.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE

invoke Invoke flag. This attribute is relevant only for ADVANCED policies

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

numpol The number of policies bound to the bindpoint.

globalBindType devno count

Example

show ssl global 1 Globally Active SSL Policy: 1)

```
    Name: certInsert_pol        Priority: 100
```

unbind ssl global

Unbinds a globally bound SSL policy.

Synopsis

unbind ssl global [-policyName <string>]

Arguments

policyName Name of the SSL policy to unbind.

type Global bind point from which the policy is to be unbound.

Possible values: CONTROL_OVERRIDE, CONTROL_DEFAULT, DATA_OVERRIDE, DATA_DEFAULT, HTTPQUIC_CONTROL_OVERRIDE, HTTPQUIC_CONTROL_DEFAULT, HTTPQUIC_DATA_OVERRIDE, HTTPQUIC_DATA_DEFAULT

priority Priority of the NOPOLICY (built-in policy) to be unbound. Not required if you are unbinding a user-defined policy. Minimum value: 1 Maximum value: 2147483647

Example

unbind ssl global -policyName certInsert_pol

ssl-hsmKey

The following operations can be performed on "ssl-hsmKey":

add| show| rm|

add ssl hsmKey

Add HSM Key.

Synopsis

add ssl hsmKey <hsmKeyName> {-password }

Arguments

hsmKeyName hsmType Type of HSM.

Possible values: THALES, SAFENET, KEYVAULT Default value: THALES

key Name of the key. optionally, for Thales, path to the HSM key file; /var/opt/nfast/kmdata/local/ is the default path. Applies when HSMTYPE is THALES or KEYVAULT. Maximum value: 63

serialNum Serial number of the partition on which the key is present. Applies only to SafeNet HSM. Maximum value: 16

password Password for a partition. Applies only to SafeNet HSM.

keystore Name of keystore object representing HSM where key is stored. For example, name of keyvault object or azurekeyvault authentication object. Applies only to KEYVAULT type HSM.

Example

add ssl hsmkey rsa1 key_simple_rsa1

show ssl hsmKey

Displays lists of all the HSM Keys Added on the Citrix ADC.

Synopsis

show ssl hsmKey

Arguments

hsmKeyName Name of the HSM Key for which to show detailed information.

Output

hsmType Type of the HSM key.

key Name of the key in HSM

serialNum SerialNum of a partition on which Safenet key is present.

keystore Store where key recides

state Current state of key

devno count stateflag

Example

An example of output of 'show ssl hsmkey' command is as shown below: sh ssl hsmkey 1 SSL HSM key: 1)SSL HSM Key Name: key_simple_rsa1

rm ssl hsmKey

Removes the specified HSM key, from the HSM Appliance.

Synopsis

rm ssl hsmKey <hsmKeyName> {-password }

Arguments

hsmKeyName Name of the HSMKEY.

hsmType Type of the HSMKEY.

Possible values: THALES, SAFENET, KEYVAULT Default value: THALES

serialNum SerialNum of a partition on which Safent HSMKey is present. Maximum value: 16

password Password of a partition on which SafeNet HSMkey is present.

Example

rm hsmkey key_simple_rsa1

ssl-keyFile

The following operations can be performed on "ssl-keyFile":

rm| show| import|

rm ssl keyFile

Deletes the specified key file.

Synopsis

rm ssl keyFile <name>

Arguments

name Name of the key file to be delete.

Example

rm ssl keyfile <name>

show ssl keyFile

Displays a list of all the imported key file objects on the Citrix ADC.

Synopsis

show ssl keyFile

Arguments

Output

name Name to assign to the imported key file. Must begin with an ASCII alphanumeric or underscore(_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

src URL specifying the protocol, host, and path, including file name, to the key file to be imported. For example, http://www.example.com/key_file. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

devno count stateflag

Example

show ssl keyfile

import ssl keyFile

Imports a key file to the Citrix ADC, assigns it a name, and stores it in the /nsconfig/ssl/keyfile folder. The folder is created if it does not exist.

Synopsis

import ssl keyFile <name> <src> {-password }

Arguments

name Name to assign to the imported key file. Must begin with an ASCII alphanumeric or underscore(_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

src URL specifying the protocol, host, and path, including file name, to the key file to be imported. For example, http://www.example.com/key_file. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

password

Example

import ssl keyfile my-keyfile http://www.example.com/key_file

ssl-logprofile

The following operations can be performed on "ssl-logprofile":

unset| show| rm| add| set|

unset ssl logprofile

Use this command to remove ssl logprofile settings.Refer to the set ssl logprofile command for meanings of the arguments.

Synopsis

unset ssl logprofile <name>

show ssl logprofile

Display all the configured SSL log profiles in the system. If a name is specified, then only that profile is shown.

Synopsis

show ssl logprofile

Arguments

name Name of the SSL log profile for which to show detailed information.

Output

sslLogClAuth log all SSL ClAuth events.

ssllogClAuthFailures log all SSL ClAuth error events.

sslLogHS log all SSL HS events.

sslLogHSfailures log all SSL HS error events.

devno count stateflag

Example

show ssl log profile

rm ssl logprofile

Remove a SSL logprofile on the Citrix ADC

Synopsis

rm ssl logprofile <name>

Arguments

name Name of the SSL log profile.

Example

rm ssllogprofile <profile name>

add ssl logprofile

Add SSL logprofile for logging SSL events.

Synopsis

add ssl logprofile <name>

Arguments

name The name of the ssllogprofile.

sslLogClAuth log all SSL ClAuth events.

Possible values: ENABLED, DISABLED Default value: DISABLED

ssllogClAuthFailures log all SSL ClAuth error events.

Possible values: ENABLED, DISABLED Default value: DISABLED

sslLogHS log all SSL HS events.

Possible values: ENABLED, DISABLED Default value: DISABLED

sslLogHSfailures log all SSL HS error events.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

add ssllogprofile <profile name>

set ssl logprofile

Set SSL logprofile for logging SSL events.

Synopsis

set ssl logprofile <name>

Arguments

name The name of the ssllogprofile.

sslLogClAuth log all SSL ClAuth events.

Possible values: ENABLED, DISABLED Default value: DISABLED

ssllogClAuthFailures log all SSL ClAuth error events.

Possible values: ENABLED, DISABLED Default value: DISABLED

sslLogHS log all SSL HS events.

Possible values: ENABLED, DISABLED Default value: DISABLED

sslLogHSfailures log all SSL HS error events.

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

set ssllogprofile <profile name> ssllog_hs_allerr ENABLE

ssl-ocspResponder

The following operations can be performed on "ssl-ocspResponder":

show| add| rm| unset| set|

show ssl ocspResponder

Displays information about all the OCSP responders configured on the appliance, or displays detailed information about the specified OCSP responder.

Synopsis

show ssl ocspResponder

Arguments

name Name of the OCSP responder for which to show detailed information.

Output

url URL of the OCSP responder.

cache Enable caching of responses. Caching of responses received from the OCSP responder enables faster responses to the clients and reduces the load on the OCSP responder.

cacheTimeout Timeout for caching the OCSP response. After the timeout, the Citrix ADC sends a fresh request to the OCSP responder for the certificate status. If a timeout is not specified, the timeout provided in the OCSP response applies.

batchingDepth Number of client certificates to batch together into one OCSP request. Batching avoids overloading the OCSP responder. A value of 1 signifies that each request is queried independently. For a value greater than 1, specify a timeout (batching delay) to avoid inordinately delaying the processing of a single certificate.

batchingDelay Maximum time, in milliseconds, to wait to accumulate OCSP requests to batch. Does not apply if the Batching Depth is 1.

ocspUrlResolveTimeout Time, in milliseconds, to wait for an OCSP URL Resolution. When this time elapses, an error message appears or the transaction is forwarded, depending on the settings on the virtual server.

resptimeout Maximum time, in mS, to wait for an OCSP response before giving up. Defaults to 2000 mS. If this is set to 0, Citrix ADC will wait for an indefinite amount of time.

producedAtTimeSkew Time, in seconds, for which the Citrix ADC waits before considering the response as invalid. The response is considered invalid if the Produced At time stamp in the OCSP response exceeds or precedes the current Citrix ADC clock time by the amount of time specified.

responderCert trustResponder A certificate to use to validate OCSP responses. Alternatively, if -trustResponder is specified, no verification will be done on the reponse. If both are omitted, only the response times (producedAt, lastUpdate, nextUpdate) will be verified.

signingCert Certificate-key pair that is used to sign OCSP requests. If this parameter is not set, the requests are not signed.

useNonce Add a nonce to the OCSP request. Protects against replay attacks.

insertClientCert Include the complete client certificate in the OCSP request.

ocspAiaRefcount No of CA certs referencing this AIA responder

httpMethod HTTP method used to send ocsp request. POST is the default httpmethod. If request length is > 255, POST wil be used even if GET is set as httpMethod

ocspIpAddrStr DNS resolved IP address.

port Port number on which OCSP Server listens.

devno count stateflag

add ssl ocspResponder

Adds an OCSP responder. An OCSP responder identifies the OCSP server that validates a certificate. Citrix ADCs support OCSP as defined in RFC 2560.

Synopsis

add ssl ocspResponder <name> -url <URL> [-cache (ENABLED | DISABLED)]

Arguments

name Name for the OCSP responder. Cannot begin with a hash (#) or space character and must contain only ASCII alphanumeric, underscore (_), hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the responder is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder" or 'my responder').

url URL of the OCSP responder.

cache Enable caching of responses. Caching of responses received from the OCSP responder enables faster responses to the clients and reduces the load on the OCSP responder.

Possible values: ENABLED, DISABLED Default value: DISABLED

cacheTimeout Timeout for caching the OCSP response. After the timeout, the Citrix ADC sends a fresh request to the OCSP responder for the certificate status. If a timeout is not specified, the timeout provided in the OCSP response applies. Default value: 1 Minimum value: 1 Maximum value: 43200

batchingDepth Number of client certificates to batch together into one OCSP request. Batching avoids overloading the OCSP responder. A value of 1 signifies that each request is queried

independently. For a value greater than 1, specify a timeout (batching delay) to avoid inordinately delaying the processing of a single certificate. Minimum value: 1 Maximum value: 8

batchingDelay Maximum time, in milliseconds, to wait to accumulate OCSP requests to batch. Does not apply if the Batching Depth is 1. Minimum value: 1 Maximum value: 10000

resptimeout Time, in milliseconds, to wait for an OCSP response. When this time elapses, an error message appears or the transaction is forwarded, depending on the settings on the virtual server. Includes Batching Delay time. Minimum value: 100 Maximum value: 120000

ocspUrlResolveTimeout Time, in milliseconds, to wait for an OCSP URL Resolution. When this time elapses, an error message appears or the transaction is forwarded, depending on the settings on the virtual server. Minimum value: 100 Maximum value: 2000

responderCert trustResponder A certificate to use to validate OCSP responses. Alternatively, if -trustResponder is specified, no verification will be done on the reponse. If both are omitted, only the response times (producedAt, lastUpdate, nextUpdate) will be verified.

producedAtTimeSkew Time, in seconds, for which the Citrix ADC waits before considering the response as invalid. The response is considered invalid if the Produced At time stamp in the OCSP response exceeds or precedes the current Citrix ADC clock time by the amount of time specified. Default value: 300 Minimum value: 0 Maximum value: 86400

signingCert Certificate-key pair that is used to sign OCSP requests. If this parameter is not set, the requests are not signed.

useNonce Enable the OCSP nonce extension, which is designed to prevent replay attacks.

Possible values: YES, NO

insertClientCert Include the complete client certificate in the OCSP request.

Possible values: YES, NO

httpMethod HTTP method used to send ocsp request. POST is the default httpmethod. If request length is > 255, POST wil be used even if GET is set as httpMethod

Possible values: GET, POST Default value: POST

Example

1. add ssl ocspResponder -url http://ocsp.example.com -producedAtTimeSkew 0 The above command will only allow responses that were generated in the same second to be used. That

is, if the response was generated at 12:00:01, it would have to be received by the Citrix ADC by 12:00:59 to be considered still valid.

2. add ssl ocspResponder -url http://ocsp.example.com -producedAtTimeSkew 300 This command will allow responses to vary up to five minutes plus or minus. That is, if the response has a producedAt time of 12:00:00, it will be accepted at the Citrix ADC if the local clock is between 11:55:00 and 12:05:00

rm ssl ocspResponder

Removes the specified OCSP responder from the appliance.

Synopsis

rm ssl ocspResponder <name> ...

Arguments

name Name of the OCSP responder to remove. The OCSP responder is removed only if it is not referenced by any other object.

Example

1)rm ssl ocspResponder o1 The above command removes the OCSP responder o1 from the system.

unset ssl ocspResponder

Removes the attributes of an OCSP responder. Attributes for which a default value is available revert to their default values. Refer to the set ssl ocspResponder command for descriptions of the arguments..Refer to the set ssl ocspResponder command for meanings of the arguments.

Synopsis

unset ssl ocspResponder <name>

set ssl ocspResponder

Modifies the parameters of an OCSP responder.

Synopsis

set ssl ocspResponder <name>

Arguments

name Name of the OCSP responder to modify.

url URL of the OCSP responder.

cache Enable caching of responses. Caching of responses received from the OCSP responder enables faster responses to the clients and reduces the load on the OCSP responder.

Possible values: ENABLED, DISABLED Default value: DISABLED

cacheTimeout Timeout for caching the OCSP response. After the timeout, the Citrix ADC sends a fresh request to the OCSP responder for the certificate status. If a timeout is not specified, the timeout provided in the OCSP response applies. Default value: 1 Minimum value: 1 Maximum value: 43200

batchingDepth Number of client certificates to batch together into one OCSP request. Batching avoids overloading the OCSP responder. A value of 1 signifies that each request is queried independently. For a value greater than 1, specify a timeout (batching delay) to avoid inordinately delaying the processing of a single certificate. Minimum value: 1 Maximum value: 8

batchingDelay Maximum time, in milliseconds, to wait to accumulate OCSP requests to batch. Does not apply if the Batching Depth is 1. Minimum value: 1 Maximum value: 10000

resptimeout Time, in milliseconds, to wait for an OCSP response. When this time elapses, an error message appears or the transaction is forwarded, depending on the settings on the virtual server. Includes Batching Delay time. Minimum value: 100 Maximum value: 120000

ocspUrlResolveTimeout Time, in milliseconds, to wait for an OCSP URL Resolution. When this time elapses, an error message appears or the transaction is forwarded, depending on the settings on the virtual server. Minimum value: 100 Maximum value: 2000

responderCert trustResponder A certificate to use to validate OCSP responses. Alternatively, if -trustResponder is specified, no verification will be done on the reponse. If both are omitted, only the response times (producedAt, lastUpdate, nextUpdate) will be verified.

producedAtTimeSkew Time, in seconds, for which the Citrix ADC waits before considering the response as invalid. The response is considered invalid if the Produced At time stamp in the OCSP response exceeds or precedes the current Citrix ADC clock time by the amount of time specified. Default value: 300 Minimum value: 0 Maximum value: 86400

signingCert Certificate-key pair that is used to sign OCSP requests. If this parameter is not set, the requests are not signed.

useNonce Enable the OCSP nonce extension, which is designed to prevent replay attacks.

Possible values: YES, NO

insertClientCert Include the complete client certificate in the OCSP request.

Possible values: YES, NO

httpMethod HTTP method used to send ocsp request. POST is the default httpmethod. If request length is > 255, POST wil be used even if GET is set as httpMethod

Possible values: GET, POST Default value: POST

Example

1. add ssl ocspResponder -url http://ocsp.example.com -producedAtTimeSkew 0 The above command will only allow responses that were generated in the same second to be used. That is, if the response was generated at 12:00:01, it would have to be received by the Citrix ADC by 12:00:59 to be considered still valid.
2. add ssl ocspResponder -url http://ocsp.example.com -producedAtTimeSkew 300 This command will allow responses to vary up to five minutes plus or minus. That is, if the response has a producedAt time of 12:00:00, it will be accepted at the Citrix ADC if the local clock is between 11:55:00 and 12:05:00

ssl-parameter

The following operations can be performed on "ssl-parameter":

set| show| unset|

set ssl parameter

Synopsis

set ssl parameter

Arguments

quantumSize Amount of data to collect before the data is pushed to the crypto hardware for encryption. For large downloads, a larger quantum size better utilizes the crypto resources.

Possible values: 4096, 8192, 16384 Default value: 8192

crlMemorySizeMB Maximum memory size to use for certificate revocation lists (CRLs). This parameter reserves memory for a CRL but sets a limit to the maximum memory that the CRLs loaded on the appliance can consume. Default value: 256 Minimum value: 10 Maximum value: 1024

strictCAChecks Enable strict CA certificate checks on the appliance.

Possible values: YES, NO Default value: NO

sslTriggerTimeout Time, in milliseconds, after which encryption is triggered for transactions that are not tracked on the Citrix ADC because their length is not known. There can be a delay of up to 10ms from the specified timeout value before the packet is pushed into the queue. Default value: 100 Minimum value: 1 Maximum value: 200

sendCloseNotify Send an SSL Close-Notify message to the client at the end of a transaction.

Possible values: YES, NO Default value: YES

encryptTriggerPktCount Maximum number of queued packets after which encryption is triggered. Use this setting for SSL transactions that send small packets from server to Citrix ADC. Default value: 45 Minimum value: 10 Maximum value: 50

denySSLReneg Deny renegotiation in specified circumstances. Available settings function as follows:

- NO - Allow SSL renegotiation.
- FRONTEND_CLIENT - Deny secure and nonsecure SSL renegotiation initiated by the client.
- FRONTEND_CLIENTSERVER - Deny secure and nonsecure SSL renegotiation initiated by the client or the Citrix ADC during policy-based client authentication.
- ALL - Deny all secure and nonsecure SSL renegotiation.
- NONSECURE - Deny nonsecure SSL renegotiation. Allows only clients that support RFC 5746.

Possible values: NO, FRONTEND_CLIENT, FRONTEND_CLIENTSERVER, ALL, NONSECURE Default value: ALL

insertionEncoding Encoding method used to insert the subject or issuer's name in HTTP requests to servers.

Possible values: Unicode, UTF-8 Default value: Unicode

ocspCacheSize Size, per packet engine, in megabytes, of the OCSP cache. A maximum of 10% of the packet engine memory can be assigned. Because the maximum allowed packet engine memory is 4GB, the maximum value that can be assigned to the OCSP cache is approximately 410 MB. Default value: 10 Minimum value: 0 Maximum value: 512

pushFlag Insert PUSH flag into decrypted, encrypted, or all records. If the PUSH flag is set to a value other than 0, the buffered records are forwarded on the basis of the value of the PUSH flag. Available settings function as follows: 0 - Auto (PUSH flag is not set.) 1 - Insert PUSH flag into every decrypted record. 2 -Insert PUSH flag into every encrypted record. 3 - Insert PUSH flag into every decrypted and encrypted record. Minimum value: 0 Maximum value: 3

dropReqWithNoHostHeader Host header check for SNI enabled sessions. If this check is enabled and the HTTP request does not contain the host header for SNI enabled sessions(i.e vserver or profile bound to vserver has SNI enabled and 'Client Hello' arrived with SNI extension), the request is dropped.

Possible values: YES, NO Default value: NO

SNIHTTPHostMatch Controls how the HTTP 'Host' header value is validated. These checks are performed only if the session is SNI enabled (i.e when vserver or profile bound to vserver has SNI enabled and 'Client Hello' arrived with SNI extension) and HTTP request contains 'Host' header. Available settings function as follows: CERT - Request is forwarded if the 'Host' value is covered by the certificate used to establish this SSL session. Note: 'CERT' matching mode cannot be applied in TLS 1.3 connections established by resuming from a previous TLS 1.3 session. On these connections, 'STRICT' matching mode will be used instead. STRICT - Request is forwarded only if value of 'Host' header in HTTP is identical to the 'Server name' value passed in 'Client Hello' of the SSL connection. NO - No validation is performed on the HTTP 'Host' header value.

Possible values: NO, CERT, STRICT Default value: CERT

pushEncTriggerTimeout PUSH encryption trigger timeout value. The timeout value is applied only if you set the Push Encryption Trigger parameter to Timer in the SSL virtual server settings. Default value: 1 Minimum value: 1 Maximum value: 200

cryptodevDisableLimit Limit to the number of disabled SSL chips after which the ADC restarts. A value of zero implies that the ADC does not automatically restart. Default value: 0 Minimum value: 0

undefActionControl Name of the undefined built-in control action: CLIENTAUTH, NOCLIENTAUTH, NOOP, RESET, or DROP. Default value: "CLIENTAUTH"

undefActionData Name of the undefined built-in data action: NOOP, RESET or DROP. Default value: "NOOP"

defaultProfile Global parameter used to enable default profile feature.

Possible values: ENABLED, DISABLED Default value: DISABLED

softwareCryptoThreshold Citrix ADC CPU utilization threshold (in percentage) beyond which crypto operations are not done in software. A value of zero implies that CPU is not utilized for doing crypto in software. Default value: 0 Minimum value: 0 Maximum value: 100

hybridFIPSMode When this mode is enabled, system will use additional crypto hardware to accelerate symmetric crypto operations.

Possible values: ENABLED, DISABLED Default value: DISABLED

sigDigestType Signature Digest Algorithms that are supported by appliance. Default value is "ALL" and it will enable the following algorithms depending on the platform. On VPX: ECDSA-SHA1 ECDSA-SHA224 ECDSA-SHA256 ECDSA-SHA384 ECDSA-SHA512 RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384 RSA-SHA512 DSA-SHA1 DSA-SHA224 DSA-SHA256 DSA-SHA384 DSA-SHA512 On MPX with Nitrox-III and coleto cards: RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384 RSA-SHA512 ECDSA-SHA1 ECDSA-SHA224 ECDSA-SHA256 ECDSA-SHA384 ECDSA-SHA512 Others: RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384 RSA-SHA512. Note:ALL doesnot include RSA-MD5 for any platform.

Default value: ALL

ssliErrorCache Enable or disable dynamically learning and caching the learned information to make the subsequent interception or bypass decision. When enabled, NS does the lookup of this cached data to do early bypass.

Possible values: ENABLED, DISABLED Default value: DISABLED

ssliMaxErrorCacheMem Specify the maximum memory that can be used for caching the learned data. This memory is used as a LRU cache so that the old entries gets replaced with new entry once the set memory limit is fully utilised. A value of 0 decides the limit automatically. Default value: 0 Minimum value: 0 Maximum value: 4294967294

insertCertSpace To insert space between lines in the certificate header of request

Possible values: YES, NO Default value: YES

ndcppComplianceCertCheck Applies when the Citrix ADC appliance acts as a client (back-end connection). Settings apply as follows: YES - During certificate verification, ignore the common name if SAN is present in the certificate. NO - Do not ignore common name.

Possible values: YES, NO Default value: NO

heterogeneousSSLHW To support both cavium and coleto based platforms in cluster environment, this mode has to be enabled.

Possible values: ENABLED, DISABLED Default value: DISABLED

operationQueueLimit Limit in percentage of capacity of the crypto operations queue beyond which new SSL connections are not accepted until the queue is reduced. Default value: 150 Minimum value: 0 Maximum value: 10000

show ssl parameter

Displays information about advanced SSL parameters.

Synopsis

show ssl parameter

Arguments

Output

quantumSize Amount of data to collect before the data is pushed to the crypto hardware for encryption. For large downloads, a larger quantum size better utilizes the crypto resources.

crlMemorySizeMB Maximum memory size to use for certificate revocation lists (CRLs). This parameter reserves memory for a CRL but sets a limit to the maximum memory that the CRLs loaded on the appliance can consume.

strictCAChecks Memory size to use for CRLs

sslTriggerTimeout Encryption trigger timer. Set the encryption trigger timeout for transactions, which are not trackable by Citrix ADC. Citrix ADC will use this setting to accumulate data received from the server for the configured time period before pushing it to the crypto hardware for encryption.

sendCloseNotify Send an SSL Close-Notify message to the client at the end of a transaction.

encryptTriggerPktCount Maximum number of queued packets after which encryption is triggered. Use this setting for SSL transactions that send small packets from server to Citrix ADC.

denySSLReneg SSL Renegotiation setting

insertionEncoding Encoding method used to insert the subject or issuer's name in HTTP requests to servers.

ocspCacheSize Size, per packet engine, in megabytes of the OCSP cache

pushFlag Insert PUSH flag into decrypted, encrypted, or all records. If the PUSH flag is set to a value other than 0, the buffered records are forwarded on the basis of the value of the PUSH flag. Available settings function as follows: 0 - Auto (PUSH flag is not set.) 1 - Insert PUSH flag into every decrypted record. 2 -Insert PUSH flag into every encrypted record. 3 - Insert PUSH flag into every decrypted and encrypted record.

dropReqWithNoHostHeader Host header check for SNI enabled sessions. If this check is enabled and the HTTP request does not contain the host header for SNI enabled sessions(i.e vserver or profile bound to vserver has SNI enabled and 'Client Hello' arrived with SNI extension), the request is dropped.

SNIHTTPHostMatch Controls how the HTTP 'Host' header value is validated. These checks are performed only if the session is SNI enabled (i.e when vserver or profile bound to vserver has SNI enabled and 'Client Hello' arrived with SNI extension) and HTTP request contains 'Host' header. Available settings function as follows: CERT - Request is forwarded if the 'Host' value is covered by the certificate used to establish this SSL session. Note: 'CERT' matching mode cannot be applied in TLS 1.3 connections established by resuming from a previous TLS 1.3 session. On these connections, 'STRICT' matching mode will be used instead. STRICT - Request is forwarded only if value of 'Host' header in HTTP is identical to the 'Server name' value passed in 'Client Hello' of the SSL connection. NO - No validation is performed on the HTTP 'Host' header value.

pushEncTriggerTimeout PUSH encryption trigger timeout value. The timeout value is applied only if you set the Push Encryption Trigger parameter to Timer in the SSL virtual server settings.

cryptodevDisableLimit Limit to the number of disabled SSL chips after which the ADC restarts. A value of zero implies that the ADC does not automatically restart.

undefActionControl Global undef action for SSL control policies

undefActionData Global undef action for SSL data policies

defaultProfile Global parameter used to enable default profile feature.

svctls1112disable Disable TLS 1.1 and 1.2 for dynamic and VPN created services.

montls1112disable Disable TLS 1.1 and 1.2 for secure (https) monitors bound to SSL_BRIDGE services.

softwareCryptoThreshold CPU quota (%) to be allocated for crypto acceleration in software. Once the CPU utilization reaches or crosses this limit, CPU won't be used for driving crypto in software.

hybridFIPSMode When this mode is enabled, system will use additional crypto hardware to accelerate symmetric crypto operations.

sigDigestType Signature Digest Algorithms that are supported by appliance. Default value is "ALL" and it will enable the following algorithms depending on the platform. On VPX: ECDSA-SHA1 ECDSA-SHA224 ECDSA-SHA256 ECDSA-SHA384 ECDSA-SHA512 RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384 RSA-SHA512 DSA-SHA1 DSA-SHA224 DSA-SHA256 DSA-SHA384 DSA-SHA512 On MPX with Nitrox-III and coleto cards: RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384 RSA-SHA512 ECDSA-SHA1 ECDSA-SHA224 ECDSA-SHA256 ECDSA-SHA384 ECDSA-SHA512 Others: RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384 RSA-SHA512. Note:ALL doesnot include RSA-MD5 for any platform.

ssliErrorCache Enable or disable dynamically learning and caching the learned information to make the subsequent interception or bypass decision. When enabled, NS does the lookup of this cached data to do early bypass.

ssliMaxErrorCacheMem Specify the maximum memory that can be used for caching the learned data. This memory is used as a LRU cache so that the old entries gets replaced with new entry once the set memory limit is fully utilised. A value of 0 decides the limit automatically.

insertCertSpace To insert space between lines in the certificate header of request

ndcppComplianceCertCheck Applies when the Citrix ADC appliance acts as a client (back-end connection). Settings apply as follows: YES - During certificate verification, ignore the common name if SAN is present in the certificate. NO - Do not ignore common name.

heterogeneousSSLHW To support both cavium and coleto based platforms in cluster environment, this mode has to be enabled.

operationQueueLimit Limit in percentage of capacity of the crypto operations queue beyond which new SSL connections are not accepted until the queue is reduced.

unset ssl parameter

Use this command to remove ssl parameter settings.Refer to the set ssl parameter command for meanings of the arguments.

Synopsis

unset ssl parameter

ssl-pkcs12

The following operations can be performed on "ssl-pkcs12":

convert ssl pkcs12

Converts the end-user certificate from PEM encoding format to PKCS#12 format. This certificate can then be distributed and installed in browsers as client certificates.

Synopsis

convert ssl pkcs12 <outfile> [-import (-des | -des3 | -aes256)] [-export] {-password } {-PEMPassPhrase }

Arguments

outfile Name for and, optionally, path to, the output file that contains the certificate and the private key after converting from PKCS#12 to PEM format. /nsconfig/ssl/ is the default path. If importing, the certificate-key pair is stored in PEM format. If exporting, the certificate-key pair is stored in PKCS#12 format. Maximum value: 63

import Convert the certificate and private-key from PKCS#12 format to PEM format.

pkcs12File Name for and, optionally, path to, the PKCS#12 file. If importing, specify the input file name that contains the certificate and the private key in PKCS#12 format. If exporting, specify the output file name that contains the certificate and the private key after converting from PEM to PKCS#12 format. /nsconfig/ssl/ is the default path. During the import operation, if the key is encrypted, you are prompted to enter the pass phrase used for encrypting the key. Maximum value: 63

des Encrypt the private key by using the DES algorithm in CBC mode during the import operation. On the command line, you are prompted to enter the pass phrase.

des3 Encrypt the private key by using the Triple-DES algorithm in EDE CBC mode (168-bit key) during the import operation. On the command line, you are prompted to enter the pass phrase.

aes256 Encrypt the private key by using the AES algorithm (256-bit key) during the import operation. On the command line, you are prompted to enter the pass phrase.

export Convert the certificate and private key from PEM format to PKCS#12 format. On the command line, you are prompted to enter the pass phrase.

certFile Certificate file to be converted from PEM to PKCS#12 format. Maximum value: 63

keyFile Name of the private key file to be converted from PEM to PKCS#12 format. If the key file is encrypted, you are prompted to enter the pass phrase used for encrypting the key. Maximum value: 63

password PEMPassPhrase

Example

1)convert ssl pkcs12 /nsconfig/ssl/client_certkey.p12 -export -cert /nsconfig/ssl/client_certcert.pem -key /nsconfig/ssl/client_key.pem The above example CLI command converts the PEM encoded certificate and key file to PKCS#12. 2)convert ssl pkcs12 /nsconfig/ssl/client_certkey.pem -import -pkcs12 /nsconfig/ssl/client_certcertkey.p12 The above example CLI command converts the PKCS12 file to PEM format. 3)convert ssl pkcs12 /nsconfig/ssl/client_certkey.pem -import -pkcs12 /nsconfig/ssl/client_certcertkey.p12 -des The above example CLI command converts the PKCS12 file to PEM format, with encrypted key.

Note:The -des option will encrypt the output key using DES algorithm. User will be prompted to enter the pass-phrase to be used for encryption.

Related Commands

- create ssl cert

ssl-pkcs8

The following operations can be performed on "ssl-pkcs8":

convert ssl pkcs8

Convert a PEM or DER format key file to PKCS#8 format before importing it into the FIPS appliance.

Synopsis

convert ssl pkcs8 <pkcs8File> <keyFile> {-password }

Arguments

pkcs8File Name for and, optionally, path to, the output file where the PKCS#8 format key file is stored. /nsconfig/ssl/ is the default path. Maximum value: 63

keyFile Name of and, optionally, path to the input key file to be converted from PEM or DER format to PKCS#8 format. /nsconfig/ssl/ is the default path. Maximum value: 63

keyform Format in which the key file is stored on the appliance.

Possible values: DER, PEM Default value: PEM

password Password to assign to the file if the key is encrypted. Applies only for PEM format files. Maximum value: 31

Example

convert ssl pkcs8 /nsconfig/ssl/key.pk8 /nsconfig/ssl/key.pem

ssl-policy

The following operations can be performed on "ssl-policy":

set| rm| add| unset| show|

set ssl policy

Modifies the parameters of an SSL policy.

Synopsis

set ssl policy <name>

Arguments

name Name of the SSL policy to modify.

rule Expression, against which traffic is evaluated.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the character.

- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the built-in or user-defined action to perform on the request. Available built-in actions are NOOP, RESET, DROP, CLIENTAUTH, NOCLIENTAUTH, INTERCEPT AND BYPASS.

undefAction Name of the action to be performed when the result of rule evaluation is undefined. Possible values for control policies: CLIENTAUTH, NOCLIENTAUTH, NOOP, RESET, DROP. Possible values for data policies: NOOP, RESET, DROP and BYPASS

comment Any comments associated with this policy.

Example

set ssl policy pol1 -rule "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh2\\")"

rm ssl policy

Removes an SSL policy.

Synopsis

rm ssl policy <name>

Arguments

name Name of the SSL policy to be removed.

Example

rm ssl policy certInsert_pol

add ssl policy

Adds an SSL policy. An SSL policy evaluates incoming traffic and applies a predefined action to requests that match a rule (expression). You have to configure the actions before creating the policies, so that you can specify an action when you create a policy.

Synopsis

add ssl policy <name> -rule <expression>

Arguments

name Name for the new SSL policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

rule Expression, against which traffic is evaluated.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the built-in or user-defined action to perform on the request. Available built-in actions are NOOP, RESET, DROP, CLIENTAUTH, NOCLIENTAUTH, INTERCEPT AND BYPASS.

undefAction Name of the action to be performed when the result of rule evaluation is undefined. Possible values for control policies: CLIENTAUTH, NOCLIENTAUTH, NOOP, RESET, DROP. Possible values for data policies: NOOP, RESET, DROP and BYPASS

comment Any comments associated with this policy.

Example

add ssl action certInsert_act -clientCert ENABLED -certHeader CERT add ssl policy certInsert_pol -rule 'HTTP.REQ.URL.STARTSWITH("/secure.html")' -reqAction certInsert_act The above example adds an SSL policy to do Client certificate insertion into the HTTP requests for any web-objects under /secure/.

unset ssl policy

Removes the attributes of an SSL policy. Attributes for which a default value is available revert to their default values. Refer to the set ssl policy command for a description of the parameters..Refer to the set ssl policy command for meanings of the arguments.

Synopsis

unset ssl policy <name>

Example

unset ssl policy pol1 -undefAction

show ssl policy

Displays information about all the SSL policies configured on the appliance, or displays detailed information about the specified SSL policy.

Synopsis

show ssl policy

Arguments

name Name of the SSL policy for which to display detailed information.

Output

stateflag rule The expression that sets the condition for application of the SSL policy.

action The name of the action to be performed on the request.

undefAction Undef Action associated with the policy.

hits Number of hits.

undefHits Number of Undef hits.

activePolicy boundTo The entity name to which policy is bound

priority gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

description Description of the policy

comment Any comments associated with this policy.

bindPolicyType vserverType peFlags type type builtin Flag to determine if SSL policy is built-in or not

feature The feature to be checked while applying this config

devno count

Example

show ssl policy 1 SSL policy: 1)

```
    Name: certInsert_pol    Rule: HTTP.REQ.URL.STARTSWITH(".html")

    Action: certInsert_act      Hits: 0
```

ssl-policylabel

The following operations can be performed on "ssl-policylabel":

bind| add| rm| show| unbind|

bind ssl policylabel

Binds an SSL policy to an SSL policy label and specifies the order in which the policies in the label are to be evaluated.

Synopsis

bind ssl policylabel <labelName> <policyName> <priority>

Arguments

labelName Name of the SSL policy label to which to bind policies.

policyName Name of the SSL policy to bind to the policy label.

priority Integer specifying the policy's priority within the label. The lower the priority number, the higher the policy's priority. Policies are evaluated in order of priority, but the order can be modified by a goto priority expression. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label. Default value: "END"

invoke Invoke policies bound to a policy label. After the invoked policies are evaluated, the flow returns to the policy with the next priority.

labelType Type of policy label invocation.

Possible values: vserver, service, policylabel

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

Example

bind ssl policylabel ssl_pol_label -policyName ssl_pol -priority 1

add ssl policylabel

Creates an SSL policy label. An SSL policy label can be a control label or a data label.

Synopsis

add ssl policylabel <labelName> -type <type>

Arguments

labelName Name for the SSL policy label. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the policy label is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my label" or 'my label').

type Type of policies that the policy label can contain.

Possible values: CONTROL, DATA, HTTPQUIC_CONTROL, HTTPQUIC_DATA

Example

add ssl policylabel ssl_pol_label -type REQ

rm ssl policylabel

Removes an SSL policy label.

Synopsis

rm ssl policylabel <labelName>

Arguments

labelName Name of the SSL policy label to remove.

Example

rm ssl policylabel ssl_pol_label

show ssl policylabel

Displays information about all the SSL policy labels, or displays detailed information about the specified policy label.

Synopsis

show ssl policylabel

Arguments

labelName Name of the SSL policy label for which to show detailed information.

Output

stateflag type Type of policies that the policy label can contain.

numpol Number of polices bound to label.

hits Number of times policy label was invoked.

policyName Name of the SSL policy to bind to the policy label.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke Invoke flag.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

flowType Flowtype of the bound SSL policy.

description Description of the policylabel

flags devno count

Example

i)show ssl policylabel ssl_pol_label ii)show ssl policylabel

unbind ssl policylabel

Unbinds an SSL policy from an SSL policy label.

Synopsis

unbind ssl policylabel <labelName> <policyName>

Arguments

labelName Name of the SSL policy label from which to unbind policies.

policyName Name of the SSL policy to unbind.

priority Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind ssl policylabel ssl_pol_label ssl_pol

ssl-profile

The following operations can be performed on "ssl-profile":

show| unbind| add| bind| rm| set| unset|

show ssl profile

Display all the configured SSL profiles in the system. If a name is specified, then only that profile is shown.

Synopsis

show ssl profile

Arguments

name Name of the SSL profile for which to show detailed information.

Output

dh State of Diffie-Hellman (DH) key exchange. This parameter is not applicable when configuring a backend profile.

dhFile The file name and path for the DH parameter.

dhCount Number of interactions, between the client and the Citrix ADC, after which the DH private-public pair is regenerated. A value of zero (0) specifies refresh every time. This parameter is not applicable when configuring a backend profile. Allowed DH count values are 0 and >= 500.

dhKeyExpSizeLimit This option enables the use of NIST recommended (NIST Special Publication 800-56A) bit size for private-key size. For example, for DH params of size 2048bit, the private-key size recommended is 224bits. This is rounded-up to 256bits.

eRSA State of Ephemeral RSA (eRSA) key exchange. Ephemeral RSA allows clients that support only export ciphers to communicate with the secure server even if the server certificate does not support export clients. The ephemeral RSA key is automatically generated when you bind an export cipher to an SSL or TCP-based SSL virtual server or service. When you remove the export cipher, the eRSA key is not deleted. It is reused at a later date when another export cipher is bound to an SSL or TCP-based SSL virtual server or service. The eRSA key is deleted when the appliance restarts. This parameter is not applicable when configuring a backend profile.

eRSACount The refresh count for the re-generation of RSA public-key and private-key pair.

sessReuse State of session reuse. Establishing the initial handshake requires CPU-intensive public key encryption operations. With the ENABLED setting, session key exchange is avoided for session resumption requests received from the client.

sessTimeout The Session timeout value in seconds.

cipherRedirect State of Cipher Redirect. If this parameter is set to ENABLED, you can configure an SSL virtual server or service to display meaningful error messages if the SSL handshake fails because of a cipher mismatch between the virtual server or service and the client. This parameter is not applicable when configuring a backend profile.

cipherURL The redirect URL to be used with the Cipher Redirect feature.

clientAuth State of client authentication. In service-based SSL offload, the service terminates the SSL handshake if the SSL client does not provide a valid certificate. This parameter is not applicable when configuring a backend profile.

clientCert The rule for client certificate requirement in client authentication.

sslRedirect State of HTTPS redirects for the SSL service. For an SSL session, if the client browser receives a redirect message, the browser tries to connect to the new location. However, the secure SSL session breaks if the object has moved from a secure site (https://) to an unsecure site (http://). Typically, a warning message appears on the screen, prompting the user to continue or disconnect. If SSL Redirect is ENABLED, the redirect message is automatically converted from http:// to https:// and the SSL session does not break. This parameter is not applicable when configuring a backend profile.

redirectPortRewrite State of the port rewrite while performing HTTPS redirect. If this parameter is set to ENABLED, and the URL from the server does not contain the standard port, the port is rewritten to the standard.

nonFipsCiphers State of usage of ciphers that are not FIPS approved. Valid only for an SSL service bound with a FIPS key and certificate.

ssl3 State of SSLv3 protocol support for the SSL profile. Note: On platforms with SSL acceleration chips, if the SSL chip does not support SSLv3, this parameter cannot be set to ENABLED.

tls1 State of TLSv1.0 protocol support for the SSL profile.

tls11 State of TLSv1.1 protocol support for the SSL profile.

tls12 State of TLSv1.2 protocol support for the SSL profile.

tls13 State of TLSv1.3 protocol support for the SSL profile.

SNIEnable State of the Server Name Indication (SNI) feature on the virtual server and service-based offload. SNI helps to enable SSL encryption on multiple domains on a single virtual server or service if the domains are controlled by the same organization and share the same second-level domain name. For example, *.sports.net can be used to secure domains such as login.sports.net and help.sports.net.

allowUnknownSNI Controls how the handshake is handled when the server name extension does not match any of the bound certificates. These checks are performed only if the session is SNI enabled (i.e. when profile bound to vserver has SNIEnable and Client Hello arrived with SNI extension). Available settings function as follows : ENABLED - handshakes with an unknown SNI are allowed to continue, if a default cert is bound. DISLABED - handshakes with an unknown SNI are not allowed to continue.

ocspStapling State of OCSP stapling support on the SSL virtual server. Supported only if the protocol used is higher than SSLv3. Possible values: ENABLED: The appliance sends a request to the OCSP responder to check the status of the server certificate and caches the response for the specified time. If the response is valid at the time of SSL handshake with the client, the OCSP-based server certificate status is sent to the client during the handshake. DISABLED: The appliance does not check the status of the server certificate.

serverAuth State of server authentication support for the SSL Backend profile.

commonName Name to be checked against the CommonName (CN) field in the server certificate bound to the SSL server.

pushEncTrigger Trigger encryption on the basis of the PUSH flag value. Available settings function as follows:

- ALWAYS - Any PUSH packet triggers encryption.
- IGNORE - Ignore PUSH packet for triggering encryption.
- MERGE - For a consecutive sequence of PUSH packets, the last PUSH packet triggers encryption.
- TIMER - PUSH packet triggering encryption is delayed by the time defined in the set ssl parameter command or in the Change Advanced SSL Settings dialog box.

sendCloseNotify Enable sending SSL Close-Notify at the end of a transaction.

clearTextPort Port on which clear-text data is sent by the appliance to the server. Do not specify this parameter for SSL offloading with end-to-end encryption.

insertionEncoding Encoding method used to insert the subject or issuer's name in HTTP requests to servers.

denySSLReneg Deny renegotiation in specified circumstances. Available settings function as follows:

- NO - Allow SSL renegotiation.
- FRONTEND_CLIENT - Deny secure and nonsecure SSL renegotiation initiated by the client.
- FRONTEND_CLIENTSERVER - Deny secure and nonsecure SSL renegotiation initiated by the client or the Citrix ADC during policy-based client authentication.
- ALL - Deny all secure and nonsecure SSL renegotiation.
- NONSECURE - Deny nonsecure SSL renegotiation. Allows only clients that support RFC 5746.

quantumSize Amount of data to collect before the data is pushed to the crypto hardware for encryption. For large downloads, a larger quantum size better utilizes the crypto resources.

strictCAChecks Enable strict CA certificate checks on the appliance.

encryptTriggerPktCount Maximum number of queued packets after which encryption is triggered. Use this setting for SSL transactions that send small packets from server to Citrix ADC.

pushFlag Insert PUSH flag into decrypted, encrypted, or all records. If the PUSH flag is set to a value other than 0, the buffered records are forwarded on the basis of the value of the PUSH flag. Available settings function as follows: 0 - Auto (PUSH flag is not set.) 1 - Insert PUSH flag into

every decrypted record. 2 -Insert PUSH flag into every encrypted record. 3 - Insert PUSH flag into every decrypted and encrypted record.

dropReqWithNoHostHeader Host header check for SNI enabled sessions. If this check is enabled and the HTTP request does not contain the host header for SNI enabled sessions(i.e vserver or profile bound to vserver has SNI enabled and 'Client Hello' arrived with SNI extension), the request is dropped.

SNIHTTPHostMatch Controls how the HTTP 'Host' header value is validated. These checks are performed only if the session is SNI enabled (i.e when vserver or profile bound to vserver has SNI enabled and 'Client Hello' arrived with SNI extension) and HTTP request contains 'Host' header. Available settings function as follows: CERT - Request is forwarded if the 'Host' value is covered by the certificate used to establish this SSL session. Note: 'CERT' matching mode cannot be applied in TLS 1.3 connections established by resuming from a previous TLS 1.3 session. On these connections, 'STRICT' matching mode will be used instead. STRICT - Request is forwarded only if value of 'Host' header in HTTP is identical to the 'Server name' value passed in 'Client Hello' of the SSL connection. NO - No validation is performed on the HTTP 'Host' header value.

pushEncTriggerTimeout PUSH encryption trigger timeout value. The timeout value is applied only if you set the Push Encryption Trigger parameter to Timer in the SSL virtual server settings.

sslTriggerTimeout Time, in milliseconds, after which encryption is triggered for transactions that are not tracked on the Citrix ADC because their length is not known. There can be a delay of up to 10ms from the specified timeout value before the packet is pushed into the queue.

eccCurveName Named ECC curve bound to vserver/service.

description The cipher suite description.

cipherAliasName/cipherName/cipherGroupName The name of the cipher group/alias/individual cipheri bindings.

cipherPriority cipher priority

cipherName The cipher group/alias/individual cipher configuration

crlCheck The state of the CRL check parameter. (Mandatory/Optional)

ocspCheck The state of the OCSP check parameter. (Mandatory/Optional)

SNICert The name of the CertKey. Use this option to bind Certkey(s) which will be used in SNI processing.

skipCAName The flag is used to indicate whether this particular CA certificate's CA_Name needs to be sent to the SSL client while requesting for client certificate in a SSL handshake

stateflag invoke Invoke flag. This attribute is relevant only for ADVANCED policies

labelType Type of policy label invocation.

sslProfileType Type of profile. Front end profiles apply to the entity that receives requests from a client. Backend profiles apply to the entity that sends client requests to a server.

gslbServiceFlag Indicates that the ssl profile has been bound to gslb service.

clientAuthUseBoundCAChain Certficates bound on the VIP are used for validating the client cert. Certficates came along with client cert are not used for validating the client cert

serviceName Service name.

ssllogProfile The name of the ssllogprofile.

service Service

builtin Flag to determine whether ssl profile is built-in or not

feature The feature to be checked while applying this config

sslpfobjecttype Internal flag to indicate what type of object binds this profile: monitor or service

sslInterception Enable or disable transparent interception of SSL sessions.

ssliCACertkey The certkey (CA certificate + private key) to be used for SSL interception.

ssliVerifyServerCertForReuse Verify the origin server's certificate before reusing the front-end SSL session. Making it hidden since we always verify for now.

ssliReneg Enable or disable triggering the client renegotiation when renegotiation request is received from the origin server.

ssliOCSPCheck Enable or disable OCSP check for origin server certificate.

ssliMaxSessPerServer Maximum ssl session to be cached per dynamic origin server. A unique ssl session is created for each SNI received from the client on ClientHello and the matching session is used for server session reuse.

sessionTicket This option enables the use of session tickets, as per the RFC 5077

sessionTicketLifeTime This option sets the life time of session tickets issued by NS in secs

sessionTicketKeyRefresh This option enables the use of session tickets, as per the RFC 5077

sessionTicketKeyData Session ticket enc/dec key , admin can set it

sessionKeyLifeTime This option sets the life time of symm key used to generate session tickets issued by NS in secs

prevSessionKeyLifeTime This option sets the life time of symm key used to generate session tickets issued by NS in secs

HSTS State of HSTS protocol support for the SSL profile. Using HSTS, a server can enforce the use of an HTTPS connection for all communication with a client

maxage Set the maximum time, in seconds, in the strict transport security (STS) header during which the client must send only HTTPS requests to the server

IncludeSubdomains Enable HSTS for subdomains. If set to Yes, a client must send only HTTPS requests for subdomains.

preload Flag indicates the consent of the site owner to have their domain preloaded.

strictSigDigestCheck Parameter indicating to check whether peer entity certificate during TLS1.2 handshake is signed with one of signature-hash combination supported by Citrix ADC.

skipClientCertPolicyCheck This flag controls the processing of X509 certificate policies. If this option is Enabled, then the policy check in Client authentication will be skipped. This option can be used only when Client Authentication is Enabled and ClientCert is set to Mandatory

zeroRttEarlyData State of TLS 1.3 0-RTT early data support for the SSL Virtual Server. This setting only has an effect if resumption is enabled, as early data cannot be sent along with an initial handshake. Early application data has significantly different security properties - in particular there is no guarantee that the data cannot be replayed.

tls13SessionTicketsPerAuthContext Number of tickets the SSL Virtual Server will issue anytime TLS 1.3 is negotiated, ticket-based resumption is enabled, and either (1) a handshake completes or (2) post-handhsake client auth completes. This value can be increased to enable clients to open multiple parallel connections using a fresh ticket for each connection. No tickets are sent if resumption is disabled.

dheKeyExchangeWithPsk Whether or not the SSL Virtual Server will require a DHE key exchange to occur when a PSK is accepted during a TLS 1.3 resumption handshake. A DHE key exchange ensures forward secrecy even in the event that ticket keys are compromised, at the expense of an additional round trip and resources required to carry out the DHE key exchange. If disabled, a DHE key exchange will be performed when a PSK is accepted but only if requested by the client. If enabled, the server will require a DHE key exchange when a PSK is accepted regardless of whether the client supports combined PSK-DHE key exchange. This setting only has an effect when resumption is enabled.

allowExtendedMasterSecret When set to YES, attempt to use the TLS Extended Master Secret (EMS, as described in RFC 7627) when negotiating TLS 1.0, TLS 1.1 and TLS 1.2 connection parameters. EMS must be supported by both the TLS client and server in order to be enabled during a handshake. This setting applies to both frontend and backend SSL profiles.

ALPNProtocol Application protocol supported by the server and used in negotiation of the protocol with the client. Possible values are HTTP1.1, HTTP2 and NONE. Default value is NONE which implies application protocol is not enabled hence remain unknown to the TLS layer. This parameter is relevant only if SSL connection is handled by the virtual server of the type SSL_TCP.

noDefaultBindings When set to YES, the SSL profile will not have default Cipher and Elliptic Curve bindings.

devno count

Example

show ssl profile

unbind ssl profile

Unbinds a cipher or eccCurve or certkey from an SSL profile.

Synopsis

unbind ssl profile <name> (-cipherName <string> | -eccCurveName <eccCurveName> | -ssliCACertkey <string>)

Arguments

name Name of the SSL profile

cipherName Name of the cipher.

eccCurveName Named ECC curve bound to service/vserver.

Possible values: ALL, P_224, P_256, P_384, P_521

ssliCACertkey The certkey (CA certificate + private key) to be used for SSL interception.

Example

unbind ssl profile ssl_profile1 -cipherName cipher_sha

add ssl profile

Add a new SSL profile on the Citrix ADC

Synopsis

add ssl profile <name> [-eRSA (ENABLED | DISABLED)] [-sessReuse (ENABLED | DISABLED)] [-cipherRedirect (ENABLED | DISABLED)] [-clientAuth (ENABLED | DISABLED)] [-SNIEnable (ENABLED | DISABLED)] {-sessionTicketKeyData }

Arguments

name Name for the SSL profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the profile is created.

sslProfileType Type of profile. Front end profiles apply to the entity that receives requests from a client. Backend profiles apply to the entity that sends client requests to a server.

Possible values: BackEnd, FrontEnd, QUIC-FrontEnd Default value: FrontEnd

ssllogProfile The name of the ssllogprofile.

dhCount Number of interactions, between the client and the Citrix ADC, after which the DH private-public pair is regenerated. A value of zero (0) specifies refresh every time. This parameter is not applicable when configuring a backend profile. Allowed DH count values are 0 and >= 500. Minimum value: 0 Maximum value: 65534

dh State of Diffie-Hellman (DH) key exchange. This parameter is not applicable when configuring a backend profile.

Possible values: ENABLED, DISABLED Default value: DISABLED

dhFile The file name and path for the DH parameter.

eRSA State of Ephemeral RSA (eRSA) key exchange. Ephemeral RSA allows clients that support only export ciphers to communicate with the secure server even if the server certificate does not support export clients. The ephemeral RSA key is automatically generated when you bind an export cipher to an SSL or TCP-based SSL virtual server or service. When you remove the export cipher, the eRSA key is not deleted. It is reused at a later date when another export cipher is bound to an SSL or TCP-based SSL virtual server or service. The eRSA key is deleted when the appliance restarts. This parameter is not applicable when configuring a backend profile.

Possible values: ENABLED, DISABLED Default value: ENABLED

eRSACount The refresh count for the re-generation of RSA public-key and private-key pair. Minimum value: 0 Maximum value: 65534

sessReuse State of session reuse. Establishing the initial handshake requires CPU-intensive public key encryption operations. With the ENABLED setting, session key exchange is avoided for session resumption requests received from the client.

Possible values: ENABLED, DISABLED Default value: ENABLED

sessTimeout The Session timeout value in seconds. Minimum value: 0 Maximum value: 4294967294

cipherRedirect State of Cipher Redirect. If this parameter is set to ENABLED, you can configure an SSL virtual server or service to display meaningful error messages if the SSL handshake fails because of a cipher mismatch between the virtual server or service and the client. This parameter is not applicable when configuring a backend profile.

Possible values: ENABLED, DISABLED Default value: DISABLED

cipherURL The redirect URL to be used with the Cipher Redirect feature.

clientAuth State of client authentication. In service-based SSL offload, the service terminates the SSL handshake if the SSL client does not provide a valid certificate. This parameter is not applicable when configuring a backend profile.

Possible values: ENABLED, DISABLED Default value: DISABLED

clientCert The rule for client certificate requirement in client authentication.

Possible values: Mandatory, Optional

dhKeyExpSizeLimit This option enables the use of NIST recommended (NIST Special Publication 800-56A) bit size for private-key size. For example, for DH params of size 2048bit, the private-key size recommended is 224bits. This is rounded-up to 256bits.

Possible values: ENABLED, DISABLED Default value: DISABLED

sslRedirect State of HTTPS redirects for the SSL service. For an SSL session, if the client browser receives a redirect message, the browser tries to connect to the new location. However, the secure SSL session breaks if the object has moved from a secure site (https://) to an unsecure site (http://). Typically, a warning message appears on the screen, prompting the user to continue or disconnect. If SSL Redirect is ENABLED, the redirect message is automatically converted from http:// to https:// and the SSL session does not break. This parameter is not applicable when configuring a backend profile.

Possible values: ENABLED, DISABLED Default value: DISABLED

redirectPortRewrite State of the port rewrite while performing HTTPS redirect. If this parameter is set to ENABLED, and the URL from the server does not contain the standard port, the port is rewritten to the standard.

Possible values: ENABLED, DISABLED Default value: DISABLED

ssl3 State of SSLv3 protocol support for the SSL profile. Note: On platforms with SSL acceleration chips, if the SSL chip does not support SSLv3, this parameter cannot be set to ENABLED.

Possible values: ENABLED, DISABLED Default value: DISABLED

tls1 State of TLSv1.0 protocol support for the SSL profile.

Possible values: ENABLED, DISABLED Default value: ENABLED

tls11 State of TLSv1.1 protocol support for the SSL profile.

Possible values: ENABLED, DISABLED Default value: ENABLED

tls12 State of TLSv1.2 protocol support for the SSL profile.

Possible values: ENABLED, DISABLED Default value: ENABLED

tls13 State of TLSv1.3 protocol support for the SSL profile.

Possible values: ENABLED, DISABLED Default value: DISABLED

SNIEnable State of the Server Name Indication (SNI) feature on the virtual server and service-based offload. SNI helps to enable SSL encryption on multiple domains on a single virtual server or service if the domains are controlled by the same organization and share the same second-level domain name. For example, *.sports.net can be used to secure domains such as login.sports.net and help.sports.net.

Possible values: ENABLED, DISABLED Default value: DISABLED

allowUnknownSNI Controls how the handshake is handled when the server name extension does not match any of the bound certificates. These checks are performed only if the session is SNI enabled (i.e. when profile bound to vserver has SNIEnable and Client Hello arrived with SNI extension). Available settings function as follows : ENABLED - handshakes with an unknown SNI are allowed to continue, if a default cert is bound. DISLABED - handshakes with an unknown SNI are not allowed to continue.

Possible values: ENABLED, DISABLED Default value: DISABLED

ocspStapling State of OCSP stapling support on the SSL virtual server. Supported only if the protocol used is higher than SSLv3. Possible values: ENABLED: The appliance sends a request to the OCSP responder to check the status of the server certificate and caches the response for the specified time. If the response is valid at the time of SSL handshake with the client, the OCSP-based server certificate status is sent to the client during the handshake. DISABLED: The appliance does not check the status of the server certificate.

Possible values: ENABLED, DISABLED Default value: DISABLED

serverAuth State of server authentication support for the SSL Backend profile.

Possible values: ENABLED, DISABLED Default value: DISABLED

commonName Name to be checked against the CommonName (CN) field in the server certificate bound to the SSL server.

pushEncTrigger Trigger encryption on the basis of the PUSH flag value. Available settings function as follows:

- ALWAYS - Any PUSH packet triggers encryption.
- IGNORE - Ignore PUSH packet for triggering encryption.
- MERGE - For a consecutive sequence of PUSH packets, the last PUSH packet triggers encryption.

- TIMER - PUSH packet triggering encryption is delayed by the time defined in the set ssl parameter command or in the Change Advanced SSL Settings dialog box.

Possible values: Always, Merge, Ignore, Timer

sendCloseNotify Enable sending SSL Close-Notify at the end of a transaction.

Possible values: YES, NO Default value: YES

clearTextPort Port on which clear-text data is sent by the appliance to the server. Do not specify this parameter for SSL offloading with end-to-end encryption.

insertionEncoding Encoding method used to insert the subject or issuer's name in HTTP requests to servers.

Possible values: Unicode, UTF-8 Default value: Unicode

denySSLReneg Deny renegotiation in specified circumstances. Available settings function as follows:

- NO - Allow SSL renegotiation.
- FRONTEND_CLIENT - Deny secure and nonsecure SSL renegotiation initiated by the client.
- FRONTEND_CLIENTSERVER - Deny secure and nonsecure SSL renegotiation initiated by the client or the Citrix ADC during policy-based client authentication.
- ALL - Deny all secure and nonsecure SSL renegotiation.
- NONSECURE - Deny nonsecure SSL renegotiation. Allows only clients that support RFC 5746.

Possible values: NO, FRONTEND_CLIENT, FRONTEND_CLIENTSERVER, ALL, NONSECURE Default value: ALL

quantumSize Amount of data to collect before the data is pushed to the crypto hardware for encryption. For large downloads, a larger quantum size better utilizes the crypto resources.

Possible values: 4096, 8192, 16384 Default value: 8192

strictCAChecks Enable strict CA certificate checks on the appliance.

Possible values: YES, NO Default value: NO

encryptTriggerPktCount Maximum number of queued packets after which encryption is triggered. Use this setting for SSL transactions that send small packets from server to Citrix ADC. Default value: 45 Minimum value: 10 Maximum value: 50

pushFlag Insert PUSH flag into decrypted, encrypted, or all records. If the PUSH flag is set to a value other than 0, the buffered records are forwarded on the basis of the value of the PUSH flag. Available settings function as follows: 0 - Auto (PUSH flag is not set.) 1 - Insert PUSH flag into every decrypted record. 2 -Insert PUSH flag into every encrypted record. 3 - Insert PUSH flag into every decrypted and encrypted record. Minimum value: 0 Maximum value: 3

dropReqWithNoHostHeader Host header check for SNI enabled sessions. If this check is enabled and the HTTP request does not contain the host header for SNI enabled sessions(i.e vserver or profile bound to vserver has SNI enabled and 'Client Hello' arrived with SNI extension), the request is dropped.

Possible values: YES, NO Default value: NO

SNIHTTPHostMatch Controls how the HTTP 'Host' header value is validated. These checks are performed only if the session is SNI enabled (i.e when vserver or profile bound to vserver has SNI enabled and 'Client Hello' arrived with SNI extension) and HTTP request contains 'Host' header. Available settings function as follows: CERT - Request is forwarded if the 'Host' value is covered by the certificate used to establish this SSL session. Note: 'CERT' matching mode cannot be applied in TLS 1.3 connections established by resuming from a previous TLS 1.3 session. On these connections, 'STRICT' matching mode will be used instead. STRICT - Request is forwarded only if value of 'Host' header in HTTP is identical to the 'Server name' value passed in 'Client Hello' of the SSL connection. NO - No validation is performed on the HTTP 'Host' header value.

Possible values: NO, CERT, STRICT Default value: CERT

pushEncTriggerTimeout PUSH encryption trigger timeout value. The timeout value is applied only if you set the Push Encryption Trigger parameter to Timer in the SSL virtual server settings. Default value: 1 Minimum value: 1 Maximum value: 200

sslTriggerTimeout Time, in milliseconds, after which encryption is triggered for transactions that are not tracked on the Citrix ADC because their length is not known. There can be a delay of up to 10ms from the specified timeout value before the packet is pushed into the queue. Default value: 100 Minimum value: 1 Maximum value: 200

clientAuthUseBoundCAChain Certficates bound on the VIP are used for validating the client cert. Certficates came along with client cert are not used for validating the client cert

Possible values: ENABLED, DISABLED Default value: DISABLED

sslInterception Enable or disable transparent interception of SSL sessions.

Possible values: ENABLED, DISABLED Default value: DISABLED

ssliReneg Enable or disable triggering the client renegotiation when renegotiation request is received from the origin server.

Possible values: ENABLED, DISABLED Default value: ENABLED

ssliOCSPCheck Enable or disable OCSP check for origin server certificate.

Possible values: ENABLED, DISABLED Default value: ENABLED

ssliMaxSessPerServer Maximum ssl session to be cached per dynamic origin server. A unique ssl session is created for each SNI received from the client on ClientHello and the matching session is used for server session reuse. Default value: 10 Minimum value: 1 Maximum value: 1000

sessionTicket This option enables the use of session tickets, as per the RFC 5077

Possible values: ENABLED, DISABLED Default value: DISABLED

sessionTicketLifeTime This option sets the life time of session tickets issued by NS in secs Default value: 300 Minimum value: 0 Maximum value: 172800

sessionTicketKeyRefresh This option enables the use of session tickets, as per the RFC 5077

Possible values: ENABLED, DISABLED Default value: ENABLED

sessionTicketKeyData Session ticket enc/dec key , admin can set it

sessionKeyLifeTime This option sets the life time of symm key used to generate session tickets issued by NS in secs Default value: 3000 Minimum value: 600 Maximum value: 86400

prevSessionKeyLifeTime This option sets the life time of symm key used to generate session tickets issued by NS in secs Default value: 0 Minimum value: 0 Maximum value: 172800

HSTS State of HSTS protocol support for the SSL profile. Using HSTS, a server can enforce the use of an HTTPS connection for all communication with a client

Possible values: ENABLED, DISABLED Default value: DISABLED

maxage Set the maximum time, in seconds, in the strict transport security (STS) header during which the client must send only HTTPS requests to the server Default value: 0 Minimum value: 0 Maximum value: 4294967294

IncludeSubdomains Enable HSTS for subdomains. If set to Yes, a client must send only HTTPS requests for subdomains.

Possible values: YES, NO Default value: NO

preload Flag indicates the consent of the site owner to have their domain preloaded.

Possible values: YES, NO Default value: NO

skipClientCertPolicyCheck This flag controls the processing of X509 certificate policies. If this option is Enabled, then the policy check in Client authentication will be skipped. This option can be used only when Client Authentication is Enabled and ClientCert is set to Mandatory

Possible values: ENABLED, DISABLED Default value: DISABLED

zeroRttEarlyData State of TLS 1.3 0-RTT early data support for the SSL Virtual Server. This setting only has an effect if resumption is enabled, as early data cannot be sent along with an initial handshake. Early application data has significantly different security properties - in particular there is no guarantee that the data cannot be replayed.

Possible values: ENABLED, DISABLED Default value: DISABLED

tls13SessionTicketsPerAuthContext Number of tickets the SSL Virtual Server will issue anytime TLS 1.3 is negotiated, ticket-based resumption is enabled, and either (1) a handshake completes or (2) post-handhsake client auth completes. This value can be increased to enable clients to open multiple parallel connections using a fresh ticket for each connection. No tickets are sent if resumption is disabled. Default value: 1 Minimum value: 1 Maximum value: 10

dheKeyExchangeWithPsk Whether or not the SSL Virtual Server will require a DHE key exchange to occur when a PSK is accepted during a TLS 1.3 resumption handshake. A DHE key exchange ensures forward secrecy even in the event that ticket keys are compromised, at the expense of an additional round trip and resources required to carry out the DHE key exchange. If disabled, a DHE key exchange will be performed when a PSK is accepted but only if requested by the client. If enabled, the server will require a DHE key exchange when a PSK is accepted regardless of whether the client supports combined PSK-DHE key exchange. This setting only has an effect when resumption is enabled.

Possible values: YES, NO Default value: NO

allowExtendedMasterSecret When set to YES, attempt to use the TLS Extended Master Secret (EMS, as described in RFC 7627) when negotiating TLS 1.0, TLS 1.1 and TLS 1.2 connection parameters. EMS must be supported by both the TLS client and server in order to be enabled during a handshake. This setting applies to both frontend and backend SSL profiles.

Possible values: YES, NO Default value: NO

ALPNProtocol Application protocol supported by the server and used in negotiation of the protocol with the client. Possible values are HTTP1.1, HTTP2 and NONE. Default value is NONE which implies application protocol is not enabled hence remain unknown to the TLS layer. This parameter is relevant only if SSL connection is handled by the virtual server of the type SSL_TCP.

Possible values: NONE, HTTP1.1, HTTP2 Default value: NONE

Example

add sslProfile <profile name> -sslProfileType FrontEnd

bind ssl profile

Binds a cipher or ecccurve or certkey to an SSL profile.

Synopsis

bind ssl profile <name> ((-cipherName <string>) | -eccCurveName <eccCurveName> | -ssliCACertkey <string>)

Arguments

name Name of the SSL profile.

cipherName Name of the cipher.

cipherPriority Priority of the cipher binding Minimum value: 1 Maximum value: 1000

eccCurveName Named ECC curve bound to service/vserver.

Possible values: ALL, P_224, P_256, P_384, P_521

ssliCACertkey The certkey (CA certificate + private key) to be used for SSL interception.

Example

1. bind ssl profile ssl_prof -cipherName cipher_sha In the above example cipher group cipher_sha is bound to the SSL profile ssl_prof. Priority of cipher_sha will be next available maximum value.
2. bind ssl profile ssl_prof -cipherName cipher_sha -cipherPriority 5 In the above example cipher group cipher_sha is bound to the SSL profile ssl_prof at cipher priority 5.
3. bind ssl profile ssl_prof -eccCurveName P_256 In the above example P_256 eccCurve is bound to the SSL profile ssl_prof.

4. bind ssl profile ssl_prof -ssliCACertkey ca_certkey In the above example the certkey named ca_certkey is bound to the SSL profile ssl_prof.

rm ssl profile

Remove a SSL profile on the Citrix ADC

Synopsis

rm ssl profile <name>

Arguments

name Name of the SSL profile.

Example

rm sslProfile <profile name>

set ssl profile

Set/modify SSL profile values

Synopsis

set ssl profile <name> [-eRSA (ENABLED | DISABLED)] [-sessReuse (ENABLED | DISABLED)] [-cipherRedirect (ENABLED | DISABLED)] [-clientAuth (ENABLED | DISABLED)] [-SNIEnable (ENABLED | DISABLED)] {-sessionTicketKeyData }

Arguments

name Name for the SSL profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the profile is created.

ssllogProfile The name of the ssllogprofile.

dh State of Diffie-Hellman (DH) key exchange. This parameter is not applicable when configuring a backend profile.

Possible values: ENABLED, DISABLED Default value: DISABLED

dhFile The file name and path for the DH parameter.

dhCount Number of interactions, between the client and the Citrix ADC, after which the DH private-public pair is regenerated. A value of zero (0) specifies refresh every time. This parameter is not applicable when configuring a backend profile. Allowed DH count values are 0 and >= 500. Minimum value: 0 Maximum value: 65534

dhKeyExpSizeLimit This option enables the use of NIST recommended (NIST Special Publication 800-56A) bit size for private-key size. For example, for DH params of size 2048bit, the private-key size recommended is 224bits. This is rounded-up to 256bits.

Possible values: ENABLED, DISABLED Default value: DISABLED

eRSA State of Ephemeral RSA (eRSA) key exchange. Ephemeral RSA allows clients that support only export ciphers to communicate with the secure server even if the server certificate does not support export clients. The ephemeral RSA key is automatically generated when you bind an export cipher to an SSL or TCP-based SSL virtual server or service. When you remove the export cipher, the eRSA key is not deleted. It is reused at a later date when another export cipher is bound to an SSL or TCP-based SSL virtual server or service. The eRSA key is deleted when the appliance restarts. This parameter is not applicable when configuring a backend profile.

Possible values: ENABLED, DISABLED Default value: ENABLED

eRSACount The refresh count for the re-generation of RSA public-key and private-key pair. Minimum value: 0 Maximum value: 65534

sessReuse State of session reuse. Establishing the initial handshake requires CPU-intensive public key encryption operations. With the ENABLED setting, session key exchange is avoided for session resumption requests received from the client.

Possible values: ENABLED, DISABLED Default value: ENABLED

sessTimeout The Session timeout value in seconds. Default value: 120 Minimum value: 0 Maximum value: 4294967294

cipherRedirect State of Cipher Redirect. If this parameter is set to ENABLED, you can configure an SSL virtual server or service to display meaningful error messages if the SSL handshake fails because of a cipher mismatch between the virtual server or service and the client. This parameter is not applicable when configuring a backend profile.

Possible values: ENABLED, DISABLED Default value: DISABLED

cipherURL The redirect URL to be used with the Cipher Redirect feature.

clientAuth State of client authentication. In service-based SSL offload, the service terminates the SSL handshake if the SSL client does not provide a valid certificate. This parameter is not applicable when configuring a backend profile.

Possible values: ENABLED, DISABLED Default value: DISABLED

clientCert The rule for client certificate requirement in client authentication.

Possible values: Mandatory, Optional

sslRedirect State of HTTPS redirects for the SSL service. For an SSL session, if the client browser receives a redirect message, the browser tries to connect to the new location. However, the secure SSL session breaks if the object has moved from a secure site (https://) to an unsecure site (http://). Typically, a warning message appears on the screen, prompting the user to continue or disconnect. If SSL Redirect is ENABLED, the redirect message is automatically converted from http:// to https:// and the SSL session does not break. This parameter is not applicable when configuring a backend profile.

Possible values: ENABLED, DISABLED Default value: DISABLED

redirectPortRewrite State of the port rewrite while performing HTTPS redirect. If this parameter is set to ENABLED, and the URL from the server does not contain the standard port, the port is rewritten to the standard.

Possible values: ENABLED, DISABLED Default value: DISABLED

ssl3 State of SSLv3 protocol support for the SSL profile. Note: On platforms with SSL acceleration chips, if the SSL chip does not support SSLv3, this parameter cannot be set to ENABLED.

Possible values: ENABLED, DISABLED Default value: DISABLED

tls1 State of TLSv1.0 protocol support for the SSL profile.

Possible values: ENABLED, DISABLED Default value: ENABLED

tls11 State of TLSv1.1 protocol support for the SSL profile.

Possible values: ENABLED, DISABLED Default value: ENABLED

tls12 State of TLSv1.2 protocol support for the SSL profile.

Possible values: ENABLED, DISABLED Default value: ENABLED

tls13 State of TLSv1.3 protocol support for the SSL profile.

Possible values: ENABLED, DISABLED Default value: DISABLED

SNIEnable State of the Server Name Indication (SNI) feature on the virtual server and service-based offload. SNI helps to enable SSL encryption on multiple domains on a single virtual server or service if the domains are controlled by the same organization and share the same second-level domain name. For example, *.sports.net can be used to secure domains such as login.sports.net and help.sports.net.

Possible values: ENABLED, DISABLED Default value: DISABLED

allowUnknownSNI Controls how the handshake is handled when the server name extension does not match any of the bound certificates. These checks are performed only if the session is SNI enabled (i.e. when profile bound to vserver has SNIEnable and Client Hello arrived with SNI extension). Available settings function as follows : ENABLED - handshakes with an unknown SNI are allowed to continue, if a default cert is bound. DISLABED - handshakes with an unknown SNI are not allowed to continue.

Possible values: ENABLED, DISABLED Default value: DISABLED

ocspStapling State of OCSP stapling support on the SSL virtual server. Supported only if the protocol used is higher than SSLv3. Possible values: ENABLED: The appliance sends a request to the OCSP responder to check the status of the server certificate and caches the response for the specified time. If the response is valid at the time of SSL handshake with the client, the OCSP-based server certificate status is sent to the client during the handshake. DISABLED: The appliance does not check the status of the server certificate.

Possible values: ENABLED, DISABLED Default value: DISABLED

serverAuth State of server authentication support for the SSL Backend profile.

Possible values: ENABLED, DISABLED Default value: DISABLED

commonName Name to be checked against the CommonName (CN) field in the server certificate bound to the SSL server.

pushEncTrigger Trigger encryption on the basis of the PUSH flag value. Available settings function as follows:

- ALWAYS - Any PUSH packet triggers encryption.
- IGNORE - Ignore PUSH packet for triggering encryption.
- MERGE - For a consecutive sequence of PUSH packets, the last PUSH packet triggers encryption.

- TIMER - PUSH packet triggering encryption is delayed by the time defined in the set ssl parameter command or in the Change Advanced SSL Settings dialog box.

Possible values: Always, Merge, Ignore, Timer

sendCloseNotify Enable sending SSL Close-Notify at the end of a transaction.

Possible values: YES, NO Default value: YES

clearTextPort Port on which clear-text data is sent by the appliance to the server. Do not specify this parameter for SSL offloading with end-to-end encryption.

insertionEncoding Encoding method used to insert the subject or issuer's name in HTTP requests to servers.

Possible values: Unicode, UTF-8 Default value: Unicode

denySSLReneg Deny renegotiation in specified circumstances. Available settings function as follows:

- NO - Allow SSL renegotiation.
- FRONTEND_CLIENT - Deny secure and nonsecure SSL renegotiation initiated by the client.
- FRONTEND_CLIENTSERVER - Deny secure and nonsecure SSL renegotiation initiated by the client or the Citrix ADC during policy-based client authentication.
- ALL - Deny all secure and nonsecure SSL renegotiation.
- NONSECURE - Deny nonsecure SSL renegotiation. Allows only clients that support RFC 5746.

Possible values: NO, FRONTEND_CLIENT, FRONTEND_CLIENTSERVER, ALL, NONSECURE Default value: ALL

quantumSize Amount of data to collect before the data is pushed to the crypto hardware for encryption. For large downloads, a larger quantum size better utilizes the crypto resources.

Possible values: 4096, 8192, 16384 Default value: 8192

strictCAChecks Enable strict CA certificate checks on the appliance.

Possible values: YES, NO Default value: NO

encryptTriggerPktCount Maximum number of queued packets after which encryption is triggered. Use this setting for SSL transactions that send small packets from server to Citrix ADC. Default value: 45 Minimum value: 10 Maximum value: 50

pushFlag Insert PUSH flag into decrypted, encrypted, or all records. If the PUSH flag is set to a value other than 0, the buffered records are forwarded on the basis of the value of the PUSH flag. Available settings function as follows: 0 - Auto (PUSH flag is not set.) 1 - Insert PUSH flag into every decrypted record. 2 -Insert PUSH flag into every encrypted record. 3 - Insert PUSH flag into every decrypted and encrypted record. Minimum value: 0 Maximum value: 3

dropReqWithNoHostHeader Host header check for SNI enabled sessions. If this check is enabled and the HTTP request does not contain the host header for SNI enabled sessions(i.e vserver or profile bound to vserver has SNI enabled and 'Client Hello' arrived with SNI extension), the request is dropped.

Possible values: YES, NO Default value: NO

SNIHTTPHostMatch Controls how the HTTP 'Host' header value is validated. These checks are performed only if the session is SNI enabled (i.e when vserver or profile bound to vserver has SNI enabled and 'Client Hello' arrived with SNI extension) and HTTP request contains 'Host' header. Available settings function as follows: CERT - Request is forwarded if the 'Host' value is covered by the certificate used to establish this SSL session. Note: 'CERT' matching mode cannot be applied in TLS 1.3 connections established by resuming from a previous TLS 1.3 session. On these connections, 'STRICT' matching mode will be used instead. STRICT - Request is forwarded only if value of 'Host' header in HTTP is identical to the 'Server name' value passed in 'Client Hello' of the SSL connection. NO - No validation is performed on the HTTP 'Host' header value.

Possible values: NO, CERT, STRICT Default value: CERT

pushEncTriggerTimeout PUSH encryption trigger timeout value. The timeout value is applied only if you set the Push Encryption Trigger parameter to Timer in the SSL virtual server settings. Default value: 1 Minimum value: 1 Maximum value: 200

sslTriggerTimeout Time, in milliseconds, after which encryption is triggered for transactions that are not tracked on the Citrix ADC because their length is not known. There can be a delay of up to 10ms from the specified timeout value before the packet is pushed into the queue. Default value: 100 Minimum value: 1 Maximum value: 200

clientAuthUseBoundCAChain Certficates bound on the VIP are used for validating the client cert. Certficates came along with client cert are not used for validating the client cert

Possible values: ENABLED, DISABLED Default value: DISABLED

sslInterception Enable or disable transparent interception of SSL sessions.

Possible values: ENABLED, DISABLED Default value: DISABLED

ssliReneg Enable or disable triggering the client renegotiation when renegotiation request is received from the origin server.

Possible values: ENABLED, DISABLED Default value: ENABLED

ssliOCSPCheck Enable or disable OCSP check for origin server certificate.

Possible values: ENABLED, DISABLED Default value: ENABLED

ssliMaxSessPerServer Maximum ssl session to be cached per dynamic origin server. A unique ssl session is created for each SNI received from the client on ClientHello and the matching session is used for server session reuse. Default value: 10 Minimum value: 1 Maximum value: 1000

HSTS State of HSTS protocol support for the SSL profile. Using HSTS, a server can enforce the use of an HTTPS connection for all communication with a client

Possible values: ENABLED, DISABLED Default value: DISABLED

maxage Set the maximum time, in seconds, in the strict transport security (STS) header during which the client must send only HTTPS requests to the server Default value: 0 Minimum value: 0 Maximum value: 4294967294

IncludeSubdomains Enable HSTS for subdomains. If set to Yes, a client must send only HTTPS requests for subdomains.

Possible values: YES, NO Default value: NO

preload Flag indicates the consent of the site owner to have their domain preloaded.

Possible values: YES, NO Default value: NO

sessionTicket This option enables the use of session tickets, as per the RFC 5077

Possible values: ENABLED, DISABLED Default value: DISABLED

sessionTicketLifeTime This option sets the life time of session tickets issued by NS in secs Default value: 300 Minimum value: 0 Maximum value: 172800

sessionTicketKeyRefresh This option enables the use of session tickets, as per the RFC 5077

Possible values: ENABLED, DISABLED Default value: ENABLED

sessionTicketKeyData Session ticket enc/dec key , admin can set it

sessionKeyLifeTime This option sets the life time of symm key used to generate session tickets issued by NS in secs Default value: 3000 Minimum value: 600 Maximum value: 86400

prevSessionKeyLifeTime This option sets the life time of symm key used to generate session tickets issued by NS in secs Default value: 0 Minimum value: 0 Maximum value: 172800

cipherName The cipher group/alias/individual cipher configuration

cipherPriority cipher priority Minimum value: 1

strictSigDigestCheck Parameter indicating to check whether peer entity certificate during TLS1.2 handshake is signed with one of signature-hash combination supported by Citrix ADC.

Possible values: ENABLED, DISABLED Default value: DISABLED

skipClientCertPolicyCheck This flag controls the processing of X509 certificate policies. If this option is Enabled, then the policy check in Client authentication will be skipped. This option can be used only when Client Authentication is Enabled and ClientCert is set to Mandatory

Possible values: ENABLED, DISABLED Default value: DISABLED

zeroRttEarlyData State of TLS 1.3 0-RTT early data support for the SSL Virtual Server. This setting only has an effect if resumption is enabled, as early data cannot be sent along with an initial handshake. Early application data has significantly different security properties - in particular there is no guarantee that the data cannot be replayed.

Possible values: ENABLED, DISABLED Default value: DISABLED

tls13SessionTicketsPerAuthContext Number of tickets the SSL Virtual Server will issue anytime TLS 1.3 is negotiated, ticket-based resumption is enabled, and either (1) a handshake completes or (2) post-handhsake client auth completes. This value can be increased to enable clients to open multiple parallel connections using a fresh ticket for each connection. No tickets are sent if resumption is disabled. Default value: 1 Minimum value: 1 Maximum value: 10

dheKeyExchangeWithPsk Whether or not the SSL Virtual Server will require a DHE key exchange to occur when a PSK is accepted during a TLS 1.3 resumption handshake. A DHE key exchange ensures forward secrecy even in the event that ticket keys are compromised, at the expense of an additional round trip and resources required to carry out the DHE key exchange. If disabled, a DHE key exchange will be performed when a PSK is accepted but only if requested by the client. If enabled, the server will require a DHE key exchange when a PSK is accepted

regardless of whether the client supports combined PSK-DHE key exchange. This setting only has an effect when resumption is enabled.

Possible values: YES, NO Default value: NO

allowExtendedMasterSecret When set to YES, attempt to use the TLS Extended Master Secret (EMS, as described in RFC 7627) when negotiating TLS 1.0, TLS 1.1 and TLS 1.2 connection parameters. EMS must be supported by both the TLS client and server in order to be enabled during a handshake. This setting applies to both frontend and backend SSL profiles.

Possible values: YES, NO Default value: NO

ALPNProtocol Application protocol supported by the server and used in negotiation of the protocol with the client. Possible values are HTTP1.1, HTTP2 and NONE. Default value is NONE which implies application protocol is not enabled hence remain unknown to the TLS layer. This parameter is relevant only if SSL connection is handled by the virtual server of the type SSL_TCP.

Possible values: NONE, HTTP1.1, HTTP2 Default value: NONE

Example

set ssl profile <profile name> -tls1 ENABLED

unset ssl profile

Use this command to remove ssl profile settings.Refer to the set ssl profile command for meanings of the arguments.

Synopsis

unset ssl profile <name>

ssl-rsakey

The following operations can be performed on "ssl-rsakey":

create ssl rsakey

Generates an RSA key.

Synopsis

create ssl rsakey <keyFile> <bits> {-password }

Arguments

keyFile Name for and, optionally, path to the RSA key file. /nsconfig/ssl/ is the default path. Maximum value: 63

bits Size, in bits, of the RSA key. Minimum value: 512 Maximum value: 4096

exponent Public exponent for the RSA key. The exponent is part of the cipher algorithm and is required for creating the RSA key.

Possible values: 3, F4 Default value: F4

keyform Format in which the RSA key file is stored on the appliance.

Possible values: DER, PEM Default value: PEM

des Encrypt the generated RSA key by using the DES algorithm. On the command line, you are prompted to enter the pass phrase (password) that is used to encrypt the key.

des3 Encrypt the generated RSA key by using the Triple-DES algorithm. On the command line, you are prompted to enter the pass phrase (password) that is used to encrypt the key.

aes256 Encrypt the generated RSA key by using the AES algorithm.

password Pass phrase to use for encryption if DES or DES3 option is selected. Maximum value: 31

pkcs8 Create the private key in PKCS#8 format.

Example

create ssl rsakey /nsconfig/ssl/rsa1024.pem 1024 -exp F4

Related Commands

- add ssl certkey

ssl-service

The following operations can be performed on "ssl-service":

bind| show| unset| set| unbind|

bind ssl service

Binds an SSL certificate-key pair or an SSL policy to a transparent SSL service.

Synopsis

bind ssl service <serviceName>@ ((-policyName <string>) | ((-certkeyName <string> [(-CA) | -SNICert]) | -cipherName <string> | -eccCurveName <eccCurveName>))

Arguments

serviceName Name of the SSL service for which to set advanced configuration.

policyName Name of the SSL policy to bind to the service.

priority Priority. Minimum value: 0 Maximum value: 64000

gotoPriorityExpression Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label. Default value: "END"

invoke Invoke policies bound to a virtual server, service, or policy label. After the invoked policies are evaluated, the flow returns to the policy with the next-larger priority number.

labelType Type of policy label invocation.

Possible values: vserver, service, policylabel

labelName Name of the policy label, virtual server, or service to invoke if the current policy rule evaluates to TRUE.

certkeyName Name of the certificate-key pair.

CA Name of the CA certificate that issues and signs the intermediate-CA certificate or the end-user client or server certificate.

crlCheck Rule to use for the CRL corresponding to the CA certificate during client authentication. Available settings function as follows:

- MANDATORY - Deny SSL clients if the CRL is missing or expired, or the Next Update date is in the past, or the CRL is incomplete.
- OPTIONAL - Allow SSL clients if the CRL is missing or expired, or the Next Update date is in the past, or the CRL is incomplete, but deny if the client certificate is revoked in the CRL.

Possible values: Mandatory, Optional

skipCAName The flag is used to indicate whether this particular CA certificate's CA_Name needs to be sent to the SSL client while requesting for client certificate in a SSL handshake

SNICert Name of the certificate-key pair to bind for use in SNI processing.

ocspCheck Rule to use for the OCSP responder associated with the CA certificate during client authentication. If MANDATORY is specified, deny all SSL clients if the OCSP check fails because of connectivity issues with the remote OCSP server, or any other reason that prevents the OCSP check. With the OPTIONAL setting, allow SSL clients even if the OCSP check fails except when the client certificate is revoked.

Possible values: Mandatory, Optional

cipherName Name of the individual cipher, user-defined cipher group, or predefined (built-in) cipher alias.

eccCurveName Named ECC curve bound to service/vserver.

Possible values: ALL, P_224, P_256, P_384, P_521

Example

bind ssl service ssl_svc -policyName certInsert_pol -priority 10

show ssl service

Displays information about SSL-specific configuration information for all SSL services, or displays detailed information about the specified SSL service.

Synopsis

show ssl service

Arguments

serviceName Name of the SSL service for which to show detailed information.

Output

crlCheck The state of the CRL check parameter. (Mandatory/Optional)

dh The state of Diffie-Hellman (DH) key exchange support.

dhFile The file name and path for the DH parameter.

dhCount The refresh count for regeneration of DH public-key and private-key from the DH parameter.

dhKeyExpSizeLimit This option enables the use of NIST recommended(NIST Special Publication 800-56A) bit size for private-key size. For example, for DH params of size 2048bit, the private-key size recommended is 224bits. This is rounded-up to 256bits.

eRSA The state of Ephemeral RSA key exchange support. Ephemeral RSA is used for export ciphers

eRSACount The refresh count for re-generation of RSA public-key and pri-vate-key pair.

sessReuse The state of session reuse support.

sessTimeout The session timeout value in seconds.

cipherRedirect The state of Cipher Redirect feature.Cipher Redirect feature can be used to provide more readable information to SSL clients about mismatch in ciphers between the client and the SSL vserver.

cipherURL The redirect URL to be used with the Cipher Redirect feature.

sslv2Redirect The state of SSLv2 Redirect feature.SSLv2 Redirect feature can be used to provide more readable information to SSL client about non-support of SSLv2 protocol on the SSL vserver.

sslv2URL The redirect URL to be used with the SSLv2 Redirect feature.

clientAuth The state of Client-Authentication support.

clientCert The rule for client certificate requirement in client authentication.

sslRedirect The state of HTTPS redirect feature.

redirectPortRewrite The state of port rewrite feature.

nonFipsCiphers The state of usage of non FIPS approved ciphers.

ssl2 The state of SSLv2 protocol support.

ssl3 The state of SSLv3 protocol support.

tls1 The state of TLSv1.0 protocol support.

tls11 The state of TLSv1.1 protocol support.

tls12 The state of TLSv1.2 protocol support.

tls13 The state of TLSv1.3 protocol support.

dtls1 The state of DTLSv1.0 protocol support.

dtls12 The state of DTLSv1.2 protocol support.

SNIEnable The state of SNI extension. Server Name Indication (SNI) helps to enable SSL encryption on multiple subdomains if the domains are controlled by the same organization and share the same second-level domain name.

ocspStapling State of OCSP stapling support on the SSL virtual server. Supported only if the protocol used is higher than SSLv3. Possible values: ENABLED: The appliance sends a request to the OCSP responder to check the status of the server certificate and caches the response for the specified time. If the response is valid at the time of SSL handshake with the client, the OCSP-based server certificate status is sent to the client during the handshake. DISABLED: The appliance does not check the status of the server certificate.

serverAuth The state of Server-Authentication support.

commonName Name to be checked against the CommonName (CN) field in the server certificate bound to the SSL server

cipherAliasName/cipherName/cipherGroupName The cipher group/alias/individual cipher configuration.

cipherName The cipher group/alias/individual cipher configuration

description The cipher suite description.

certkeyName The certificate key pair binding.

policyName The SSL policy binding.

invoke Invoke flag. This attribute is relevant only for ADVANCED policies

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

clearTextPort The clearTextPort settings.

service priority The priority of the policies bound to this SSL service

polinherit Whether the bound policy is a inherited policy or not

ocspCheck Rule to use for the OCSP responder associated with the CA certificate during client authentication. If MANDATORY is specified, deny all SSL clients if the OCSP check fails because of connectivity issues with the remote OCSP server, or any other reason that prevents the OCSP check. With the OPTIONAL setting, allow SSL clients even if the OCSP check fails except when the client certificate is revoked.

pushEncTrigger PUSH packet triggering encryption: Always, Ignore, Merge

CA CA certificate.

SNICert The name of the CertKey. Use this option to bind Certkey(s) which will be used in SNI processing.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

stateflag skipCAName The flag is used to indicate whether this particular CA certificate's CA_Name needs to be sent to the SSL client while requesting for client certificate in a SSL handshake

sendCloseNotify Enable sending SSL Close-Notify at the end of a transaction

dtlsProfileName Name of the DTLS profile that contains DTLS settings for the service.

dtlsFlag The flag is used to indicate whether DTLS is set or not

quicFlag eccCurveName Named ECC curve bound to service/vserver.

sslProfile Name of the SSL profile that contains SSL settings for the service.

gslbServiceFlag Indicates that this is a gslb service

strictSigDigestCheck Parameter indicating to check whether peer's certificate during TLS1.2 handshake is signed with one of signature-hash combination supported by Citrix ADC

cipherDefaultOn Flag indicating whether the bound cipher was the DEFAULT cipher, bound at boot time, or any other cipher from the CLI

devno count

Example

An example of output of show ssl service command is as shown below show ssl service svc1

```
    Advanced SSL configuration for Back-end SSL Service svc1:

    DH: DISABLED

    Ephemeral RSA: ENABLED          Refresh Count: 0

    Session Reuse: ENABLED          Timeout: 300 seconds

    Cipher Redirect: DISABLED

    SSLv2 Redirect: DISABLED

    Server Auth: DISABLED

    SSL Redirect: DISABLED

    Non FIPS Ciphers: DISABLED

    SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED
```

```
1)      Cipher Name: ALL

Description: Predefined Cipher Alias
```

unset ssl service

Use this command to remove ssl service settings.Refer to the set ssl service command for meanings of the arguments.

Synopsis

unset ssl service <serviceName>@

set ssl service

Sets the advanced SSL configuration for an SSL service.

Synopsis

set ssl service <serviceName>@ [-eRSA (ENABLED | DISABLED)] [-sessReuse (ENABLED | DISABLED)] [-cipherRedirect (ENABLED | DISABLED)] [-sslv2Redirect (ENABLED | DISABLED)] [-clientAuth (ENABLED | DISABLED)]

Arguments

serviceName Name of the SSL service.

dh State of Diffie-Hellman (DH) key exchange. This parameter is not applicable when configuring a backend service.

Possible values: ENABLED, DISABLED Default value: DISABLED

dhFile Name for and, optionally, path to the PEM-format DH parameter file to be installed. /nsconfig/ssl/ is the default path. This parameter is not applicable when configuring a backend service.

dhCount Number of interactions, between the client and the Citrix ADC, after which the DH private-public pair is regenerated. A value of zero (0) specifies refresh every time. This parameter is not applicable when configuring a backend service. Allowed DH count values are 0 and >= 500. Minimum value: 0 Maximum value: 65534

dhKeyExpSizeLimit This option enables the use of NIST recommended (NIST Special Publication 800-56A) bit size for private-key size. For example, for DH params of size 2048bit, the private-key size recommended is 224bits. This is rounded-up to 256bits.

Possible values: ENABLED, DISABLED Default value: DISABLED

eRSA State of Ephemeral RSA (eRSA) key exchange. Ephemeral RSA allows clients that support only export ciphers to communicate with the secure server even if the server certificate does not support export clients. The ephemeral RSA key is automatically generated when you bind an export cipher to an SSL or TCP-based SSL virtual server or service. When you remove the export cipher, the eRSA key is not deleted. It is reused at a later date when another export cipher is bound to an SSL or TCP-based SSL virtual server or service. The eRSA key is deleted when the appliance restarts. This parameter is not applicable when configuring a backend service.

Possible values: ENABLED, DISABLED Default value: DISABLED

eRSACount Refresh count for regeneration of RSA public-key and private-key pair. Zero (0) specifies infinite usage (no refresh). This parameter is not applicable when configuring a backend service. Minimum value: 0 Maximum value: 65534

sessReuse State of session reuse. Establishing the initial handshake requires CPU-intensive public key encryption operations. With the ENABLED setting, session key exchange is avoided for session resumption requests received from the client.

Possible values: ENABLED, DISABLED Default value: ENABLED

sessTimeout Time, in seconds, for which to keep the session active. Any session resumption request received after the timeout period will require a fresh SSL handshake and establishment of a new SSL session. Default value: 300 Minimum value: 0 Maximum value: 4294967294

cipherRedirect State of Cipher Redirect. If this parameter is set to ENABLED, you can configure an SSL virtual server or service to display meaningful error messages if the SSL handshake fails because of a cipher mismatch between the virtual server or service and the client. This parameter is not applicable when configuring a backend service.

Possible values: ENABLED, DISABLED Default value: DISABLED

cipherURL URL of the page to which to redirect the client in case of a cipher mismatch. Typically, this page has a clear explanation of the error or an alternative location that the transaction can continue from. This parameter is not applicable when configuring a backend service.

sslv2Redirect State of SSLv2 Redirect. If this parameter is set to ENABLED, you can configure an SSL virtual server or service to display meaningful error messages if the SSL handshake fails because of a protocol version mismatch between the virtual server or service and the client. This parameter is not applicable when configuring a backend service.

Possible values: ENABLED, DISABLED Default value: DISABLED

sslv2URL URL of the page to which to redirect the client in case of a protocol version mismatch. Typically, this page has a clear explanation of the error or an alternative location that the transaction can continue from. This parameter is not applicable when configuring a backend service.

clientAuth State of client authentication. In service-based SSL offload, the service terminates the SSL handshake if the SSL client does not provide a valid certificate. This parameter is not applicable when configuring a backend service.

Possible values: ENABLED, DISABLED Default value: DISABLED

clientCert Type of client authentication. If this parameter is set to MANDATORY, the appliance terminates the SSL handshake if the SSL client does not provide a valid certificate. With the OPTIONAL setting, the appliance requests a certificate from the SSL clients but proceeds with the SSL transaction even if the client presents an invalid certificate. This parameter is not applicable when configuring a backend SSL service. Caution: Define proper access control policies before changing this setting to Optional.

Possible values: Mandatory, Optional

sslRedirect State of HTTPS redirects for the SSL service.

For an SSL session, if the client browser receives a redirect message, the browser tries to connect to the new location. However, the secure SSL session breaks if the object has moved from a secure site (https://) to an unsecure site (http://). Typically, a warning message appears on the screen, prompting the user to continue or disconnect. If SSL Redirect is ENABLED, the redirect message is automatically converted from http:// to https:// and the SSL session does not break.

This parameter is not applicable when configuring a backend service.

Possible values: ENABLED, DISABLED Default value: DISABLED

redirectPortRewrite State of the port rewrite while performing HTTPS redirect. If this parameter is set to ENABLED, and the URL from the server does not contain the standard port, the port is rewritten to the standard.

Possible values: ENABLED, DISABLED Default value: DISABLED

ssl2 State of SSLv2 protocol support for the SSL service. This parameter is not applicable when configuring a backend service.

Possible values: ENABLED, DISABLED Default value: DISABLED

ssl3 State of SSLv3 protocol support for the SSL service. Note: On platforms with SSL acceleration chips, if the SSL chip does not support SSLv3, this parameter cannot be set to ENABLED.

Possible values: ENABLED, DISABLED Default value: ENABLED

tls1 State of TLSv1.0 protocol support for the SSL service.

Possible values: ENABLED, DISABLED Default value: ENABLED

tls11 State of TLSv1.1 protocol support for the SSL service.

Possible values: ENABLED, DISABLED Default value: ENABLED

tls12 State of TLSv1.2 protocol support for the SSL service.

Possible values: ENABLED, DISABLED Default value: ENABLED

tls13 State of TLSv1.3 protocol support for the SSL service.

Possible values: ENABLED, DISABLED Default value: DISABLED

dtls1 State of DTLSv1.0 protocol support for the SSL service.

Possible values: ENABLED, DISABLED Default value: ENABLED

dtls12 State of DTLSv1.2 protocol support for the SSL service.

Possible values: ENABLED, DISABLED Default value: DISABLED

SNIEnable State of the Server Name Indication (SNI) feature on the virtual server and service-based offload. SNI helps to enable SSL encryption on multiple domains on a single virtual server or service if the domains are controlled by the same organization and share the same second-level domain name. For example, *.sports.net can be used to secure domains such as login.sports.net and help.sports.net.

Possible values: ENABLED, DISABLED Default value: DISABLED

ocspStapling State of OCSP stapling support on the SSL virtual server. Supported only if the protocol used is higher than SSLv3. Possible values: ENABLED: The appliance sends a request to the OCSP responder to check the status of the server certificate and caches the response for the specified time. If the response is valid at the time of SSL handshake with the client, the OCSP-based server certificate status is sent to the client during the handshake. DISABLED: The appliance does not check the status of the server certificate.

Possible values: ENABLED, DISABLED Default value: DISABLED

serverAuth State of server authentication support for the SSL service.

Possible values: ENABLED, DISABLED Default value: DISABLED

commonName Name to be checked against the CommonName (CN) field in the server certificate bound to the SSL server

pushEncTrigger Trigger encryption on the basis of the PUSH flag value. Available settings function as follows:

- ALWAYS - Any PUSH packet triggers encryption.
- IGNORE - Ignore PUSH packet for triggering encryption.
- MERGE - For a consecutive sequence of PUSH packets, the last PUSH packet triggers encryption.
- TIMER - PUSH packet triggering encryption is delayed by the time defined in the set ssl parameter command or in the Change Advanced SSL Settings dialog box.

Possible values: Always, Merge, Ignore, Timer

sendCloseNotify Enable sending SSL Close-Notify at the end of a transaction

Possible values: YES, NO Default value: YES

dtlsProfileName Name of the DTLS profile that contains DTLS settings for the service.

sslProfile Name of the SSL profile that contains SSL settings for the service.

strictSigDigestCheck Parameter indicating to check whether peer's certificate during TLS1.2 handshake is signed with one of signature-hash combination supported by Citrix ADC

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

1)set ssl service sslsvc -dh ENABLED -dhFile /nsconfig/ssl/dh1024.pem -dhCount 500 The above example sets the DH parameters for the SSL service 'sslsvc'. 2.set ssl service sslsvc -ssl2 DISABLED The above example disables the support for SSLv2 protocol for the SSL service 'sslsvc'.

unbind ssl service

Unbinds an SSL policy, cipher, and certificate-key pair from an SSL service.

Synopsis

unbind ssl service <serviceName>@ ((-policyName <string>) | ((-certkeyName <string> [(-CA) | -SNICert]) | -cipherName <string> | -eccCurveName <eccCurveName>))

Arguments

serviceName Name of the SSL service.

policyName Name of the SSL policy to unbind from the SSL service.

priority Priority of the NOPOLICY (built-in policy) to be unbound. Not required if you are unbinding a user-defined policy. Minimum value: 1 Maximum value: 2147483647

certkeyName The certificate key pair binding.

CA CA certificate.

crlCheck Rule to use for the CRL corresponding to the CA certificate during client authentication. Available settings function as follows:

- MANDATORY - Deny SSL clients if the CRL is missing or expired, or the Next Update date is in the past, or the CRL is incomplete.
- OPTIONAL - Allow SSL clients if the CRL is missing or expired, or the Next Update date is in the past, or the CRL is incomplete, but deny if the client certificate is revoked in the CRL.

Possible values: Mandatory, Optional

SNICert Name of the certificate-key pair to bind for use in SNI processing.

cipherName Name of the individual cipher, user-defined cipher group, or predefined (built-in) cipher alias.

eccCurveName Named ECC curve bound to service/vserver.

Possible values: ALL, P_224, P_256, P_384, P_521

Example

unbind ssl service ssl_svc -policyName certInsert_pol

ssl-serviceGroup

The following operations can be performed on "ssl-serviceGroup":

set| unbind| bind| show| unset|

set ssl serviceGroup

Sets the advanced SSL configuration for an SSL service group.

Synopsis

set ssl serviceGroup <serviceGroupName>@ [-sessReuse (ENABLED | DISABLED)]

Arguments

serviceGroupName Name of the SSL service group for which to set advanced configuration.

sslProfile Name of the SSL profile that contains SSL settings for the Service Group.

sessReuse State of session reuse. Establishing the initial handshake requires CPU-intensive public key encryption operations. With the ENABLED setting, session key exchange is avoided for session resumption requests received from the client.

Possible values: ENABLED, DISABLED Default value: ENABLED

sessTimeout Time, in seconds, for which to keep the session active. Any session resumption request received after the timeout period will require a fresh SSL handshake and establishment of a new SSL session. Default value: 300 Minimum value: 0 Maximum value: 4294967294

ssl3 State of SSLv3 protocol support for the SSL service group. Note: On platforms with SSL acceleration chips, if the SSL chip does not support SSLv3, this parameter cannot be set to ENABLED.

Possible values: ENABLED, DISABLED Default value: ENABLED

tls1 State of TLSv1.0 protocol support for the SSL service group.

Possible values: ENABLED, DISABLED Default value: ENABLED

tls11 State of TLSv1.1 protocol support for the SSL service group.

Possible values: ENABLED, DISABLED Default value: ENABLED

tls12 State of TLSv1.2 protocol support for the SSL service group.

Possible values: ENABLED, DISABLED Default value: ENABLED

tls13 State of TLSv1.3 protocol support for the SSL service group.

Possible values: ENABLED, DISABLED Default value: DISABLED

SNIEnable State of the Server Name Indication (SNI) feature on the service. SNI helps to enable SSL encryption on multiple domains on a single virtual server or service if the domains are controlled by the same organization and share the same second-level domain name. For example, *.sports.net can be used to secure domains such as login.sports.net and help.sports.net.

Possible values: ENABLED, DISABLED Default value: DISABLED

ocspStapling State of OCSP stapling support on the SSL virtual server. Supported only if the protocol used is higher than SSLv3. Possible values: ENABLED: The appliance sends a request to the OCSP responder to check the status of the server certificate and caches the response for the specified time. If the response is valid at the time of SSL handshake with the client, the OCSP-based server certificate status is sent to the client during the handshake. DISABLED: The appliance does not check the status of the server certificate.

Possible values: ENABLED, DISABLED Default value: DISABLED

serverAuth State of server authentication support for the SSL service group.

Possible values: ENABLED, DISABLED Default value: DISABLED

commonName Name to be checked against the CommonName (CN) field in the server certificate bound to the SSL server

sendCloseNotify Enable sending SSL Close-Notify at the end of a transaction

Possible values: YES, NO Default value: YES

strictSigDigestCheck Parameter indicating to check whether peer's certificate is signed with one of signature-hash combination supported by Citrix ADC

Possible values: ENABLED, DISABLED Default value: DISABLED

Example

1)set ssl servicegroup svcg1 -sessReuse DISABLED The above example disables session reuse for the service group 'svcg1'.

unbind ssl serviceGroup

Unbind a SSL policy from a SSL service.

Synopsis

unbind ssl serviceGroup <serviceGroupName>@ ((-certkeyName <string> [(-CA) | -SNICert]) | -cipherName <string>)

Arguments

serviceGroupName The name of the SSL service from which the SSL policy needs to be unbound.

certkeyName The name of the certificate bound to the SSL service group.

CA CA certificate.

crlCheck The rule for use of CRL corresponding to this CA certificate during client authentication. If crlCheck is set to Mandatory, the system will deny all SSL clients if the CRL is missing, expired - NextUpdate date is in the past, or is incomplete with remote CRL refresh enabled. If crlCheck is set to optional, the system will allow SSL clients in the above error cases.However, in any case if the client certificate is revoked in the CRL, the SSL client will be denied access.

Possible values: Mandatory, Optional

SNICert The name of the CertKey. Use this option to bind Certkey(s) which will be used in SNI processing.

cipherName A cipher-suite can consist of an individual cipher name, the system predefined cipher-alias name, or user defined cipher-group name.

eccCurveName Named ECC curve bound to service group

Possible values: ALL, P_224, P_256, P_384, P_521

Example

unbind ssl service ssl_svc -policyName certInsert_pol

bind ssl serviceGroup

Bind a SSL certkey or a SSL policy to a SSL service.

Synopsis

bind ssl serviceGroup <serviceGroupName>@ ((-certkeyName <string> [(-CA) | -SNICert]) | -cipherName <string>)

Arguments

serviceGroupName The name of the SSL service to which the SSL policy needs to be bound.

certkeyName The name of the CertKey

CA CA certificate.

crlCheck The rule for use of CRL corresponding to this CA certificate during client authentication. If crlCheck is set to Mandatory, the system will deny all SSL clients if the CRL is missing, expired - NextUpdate date is in the past, or is incomplete with remote CRL refresh enabled. If crlCheck is set to optional, the system will allow SSL clients in the above error cases.However, in any case if the client certificate is revoked in the CRL, the SSL client will be denied access.

Possible values: Mandatory, Optional

SNICert The name of the CertKey. Use this option to bind Certkey(s) which will be used in SNI processing.

ocspCheck The state of the OCSP check parameter. (Mandatory/Optional)

Possible values: Mandatory, Optional

cipherName A cipher-suite can consist of an individual cipher name, the system predefined cipher-alias name, or user defined cipher-group name.

eccCurveName Named ECC curve bound to service group

Possible values: ALL, P_224, P_256, P_384, P_521

Example

bind ssl service ssl_svc -policyName certInsert_pol -priority 10

show ssl serviceGroup

Displays information about SSL-specific configuration for all SSL service groups, or displays detailed information about the specified SSL service group.

Synopsis

show ssl serviceGroup

Arguments

serviceGroupName Name of the SSL service group for which to show detailed information.

Output

dh The state of DH key exchange support for the SSL service group.

dhFile The file name and path for the DH parameter.

dhCount The refresh count for the re-generation of DH public-key and private-key from the DH parameter.

dhKeyExpSizeLimit This option enables the use of NIST recommended (NIST Special Publication 800-56A) bit size for private-key size. For example, for DH params of size 2048bit, the private-key size recommended is 224bits. This is rounded-up to 256bits.

eRSA The state of Ephemeral RSA key exchange support for the SSL service group.Ephemeral RSA is used for export ciphers.

eRSACount The refresh count for the re-generation of RSA public-key and private-key pair.

sessReuse The state of session re-use support for the SSL service group.

sessTimeout The Session timeout value in seconds.

cipherRedirect The state of Cipher Redirect feature. Cipher Redirect feature can be used to provide more readable information to SSL clients about mismatch in ciphers between the client and the SSL vserver.

cipherURL The redirect URL to be used with the Cipher Redirect feature.

sslv2Redirect The state of SSLv2 Redirect feature.SSLv2 Redirect feature can be used to provide more readable information to SSL client about non-support of SSLv2 protocol on the SSL vserver.

sslv2URL The redirect URL to be used with SSLv2 Redirect feature.

clientAuth The state of Client-Authentication support for the SSL service group.

clientCert The rule for client certificate requirement in client authentication.

sslRedirect The state of HTTPS redirects for the SSL service group.

This is required for the proper functioning of the redirect messages from the server. The redirect message from the server provides the new location for the moved object. This is contained in the HTTP header field: Location, e.g. Location: http://www.moved.org/here.html

For the SSL session, if the client browser receives this message, the browser will try to connect to the new location. This will break the secure SSL session, as the object has moved from a secure site (https://) to an un-secure one (http://). Generally browsers flash a warning message on the screen and prompt the user, either to continue or disconnect.

The above feature, when enabled will automatically convert all such http:// redirect message to https://. This will not break the client SSL session.

Note: The set ssl service command can be used for configuring a front-end SSL service for service based SSL Off-Loading, or a backend SSL service for backend-encryption setup.

redirectPortRewrite The state of port-rewrite feature.

nonFipsCiphers The state of usage of non FIPS approved ciphers.

ssl2 The state of SSLv2 protocol support for the SSL service group.

ssl3 State of SSLv3 protocol support for the SSL service group. Note: On platforms with SSL acceleration chips, if the SSL chip does not support SSLv3, this parameter cannot be set to ENABLED.

tls1 State of TLSv1.0 protocol support for the SSL service group.

tls11 State of TLSv1.1 protocol support for the SSL service group.

tls12 State of TLSv1.2 protocol support for the SSL service group.

tls13 State of TLSv1.3 protocol support for the SSL service group.

SNIEnable The state of SNI extension. Server Name Indication (SNI) helps to enable SSL encryption on multiple subdomains if the domains are controlled by the same organization and share the same second-level domain name.

ocspStapling State of OCSP stapling support on the SSL virtual server. Supported only if the protocol used is higher than SSLv3. Possible values: ENABLED: The appliance sends a request to the OCSP responder to check the status of the server certificate and caches the response for the specified time. If the response is valid at the time of SSL handshake with the client, the OCSP-based server certificate status is sent to the client during the handshake. DISABLED: The appliance does not check the status of the server certificate.

serverAuth The state of the server authentication configuration for the SSL service group. For SSL deployments where data is encrypted end-to-end using SSL, you can authenticate the server.

commonName Name to be checked against the CommonName (CN) field in the server certificate bound to the SSL server

cipherAliasName/cipherName/cipherGroupName The name of the cipher group/alias/name configured for the SSL service group.

cipherName The name of the cipher group/alias/name configured for the SSL service group.

ocspCheck The state of the OCSP check parameter. (Mandatory/Optional)

crlCheck The state of the CRL check parameter. (Mandatory/Optional)

description The description of the cipher.

certkeyName The name of the certificate bound to the SSL service group.

clearTextPort The port on the back-end web-servers where the clear-text data is sent by system. Use this setting for the wildcard IP based SSL Acceleration configuration (*:443).

serviceName The service name.

CA CA certificate.

SNICert The name of the CertKey. Use this option to bind Certkey(s) which will be used in SNI processing.

stateflag sendCloseNotify Enable sending SSL Close-Notify at the end of a transaction

eccCurveName Named ECC curve bound to servicegroup.

sslProfile Name of the SSL profile that contains SSL settings for the Service Group.

strictSigDigestCheck Parameter indicating to check whether peer's certificate is signed with one of signature-hash combination supported by Citrix ADC

service servicegroup devno count

Example

An example of output of show ssl servicegroup command is as shown below show ssl servicegroup ssl_svcg

```
Advanced SSL configuration for Back-end SSL Service Group ssl_svcg:

Session Reuse: ENABLED          Timeout: 300 seconds

Server Auth: DISABLED

Non FIPS Ciphers: DISABLED

SSLv3: ENABLED  TLSv1: ENABLED
```

1. ```
   Cipher Name: ALL

   Description: Predefined Cipher Alias
   ```

unset ssl serviceGroup

Use this command to remove ssl serviceGroup settings.Refer to the set ssl serviceGroup command for meanings of the arguments.

Synopsis

unset ssl serviceGroup <serviceGroupName>@

ssl-stats

The following operations can be performed on "ssl-stats":

show ssl stats

show ssl stats is an alias for stat ssl

Synopsis

show ssl stats - alias for 'stat ssl'
   ```

ssl-vserver

The following operations can be performed on "ssl-vserver":

unset| set| bind| unbind| show| stat|

unset ssl vserver

Use this command to remove ssl vserver settings.Refer to the set ssl vserver command for meanings of the arguments.

Synopsis

unset ssl vserver <vServerName>@

set ssl vserver

Sets advanced SSL configuration for an SSL virtual server.

Synopsis

set ssl vserver <vServerName>@ [-eRSA (ENABLED | DISABLED)] [-sessReuse (ENABLED | DISABLED)] [-cipherRedirect (ENABLED | DISABLED)] [-sslv2Redirect (ENABLED | DISABLED)] [-clientAuth (ENABLED | DISABLED)]

Arguments

vServerName Name of the SSL virtual server for which to set advanced configuration.

clearTextPort Port on which clear-text data is sent by the appliance to the server. Do not specify this parameter for SSL offloading with end-to-end encryption. Default value: 0 Maximum value: 65534

dh State of Diffie-Hellman (DH) key exchange.

Possible values: ENABLED, DISABLED Default value: DISABLED

dhFile Name of and, optionally, path to the DH parameter file, in PEM format, to be installed. /nsconfig/ssl/ is the default path.

dhCount Number of interactions, between the client and the Citrix ADC, after which the DH private-public pair is regenerated. A value of zero (0) specifies refresh every time. Minimum value: 0 Maximum value: 65534

dhKeyExpSizeLimit This option enables the use of NIST recommended (NIST Special Publication 800-56A) bit size for private-key size. For example, for DH params of size 2048bit, the private-key size recommended is 224bits. This is rounded-up to 256bits.

Possible values: ENABLED, DISABLED Default value: DISABLED

eRSA State of Ephemeral RSA (eRSA) key exchange. Ephemeral RSA allows clients that support only export ciphers to communicate with the secure server even if the server certificate does not support export clients. The ephemeral RSA key is automatically generated when you bind an export cipher to an SSL or TCP-based SSL virtual server or service. When you remove the export cipher, the eRSA key is not deleted. It is reused at a later date when another export cipher is bound to an SSL or TCP-based SSL virtual server or service. The eRSA key is deleted when the appliance restarts.

Possible values: ENABLED, DISABLED Default value: ENABLED

eRSACount Refresh count for regeneration of the RSA public-key and private-key pair. Zero (0) specifies infinite usage (no refresh). Minimum value: 0 Maximum value: 65534

sessReuse State of session reuse. Establishing the initial handshake requires CPU-intensive public key encryption operations. With the ENABLED setting, session key exchange is avoided for session resumption requests received from the client.

Possible values: ENABLED, DISABLED Default value: ENABLED

sessTimeout Time, in seconds, for which to keep the session active. Any session resumption request received after the timeout period will require a fresh SSL handshake and establishment of a new SSL session. Default value: 120 Minimum value: 0 Maximum value: 4294967294

cipherRedirect State of Cipher Redirect. If cipher redirect is enabled, you can configure an SSL virtual server or service to display meaningful error messages if the SSL handshake fails because of a cipher mismatch between the virtual server or service and the client.

Possible values: ENABLED, DISABLED Default value: DISABLED

cipherURL The redirect URL to be used with the Cipher Redirect feature.

sslv2Redirect State of SSLv2 Redirect. If SSLv2 redirect is enabled, you can configure an SSL virtual server or service to display meaningful error messages if the SSL handshake fails because of a protocol version mismatch between the virtual server or service and the client.

Possible values: ENABLED, DISABLED Default value: DISABLED

sslv2URL URL of the page to which to redirect the client in case of a protocol version mismatch. Typically, this page has a clear explanation of the error or an alternative location that the transaction can continue from.

clientAuth State of client authentication. If client authentication is enabled, the virtual server terminates the SSL handshake if the SSL client does not provide a valid certificate.

Possible values: ENABLED, DISABLED Default value: DISABLED

clientCert Type of client authentication. If this parameter is set to MANDATORY, the appliance terminates the SSL handshake if the SSL client does not provide a valid certificate. With the OPTIONAL setting, the appliance requests a certificate from the SSL clients but proceeds with the SSL transaction even if the client presents an invalid certificate. Caution: Define proper access control policies before changing this setting to Optional.

Possible values: Mandatory, Optional

sslRedirect State of HTTPS redirects for the SSL virtual server.

For an SSL session, if the client browser receives a redirect message, the browser tries to connect to the new location. However, the secure SSL session breaks if the object has moved from a secure site (https://) to an unsecure site (http://). Typically, a warning message appears on the screen, prompting the user to continue or disconnect. If SSL Redirect is ENABLED, the redirect message is automatically converted from http:// to https:// and the SSL session does not break.

Possible values: ENABLED, DISABLED Default value: DISABLED

redirectPortRewrite State of the port rewrite while performing HTTPS redirect. If this parameter is ENABLED and the URL from the server does not contain the standard port, the port is rewritten to the standard.

Possible values: ENABLED, DISABLED Default value: DISABLED

ssl2 State of SSLv2 protocol support for the SSL Virtual Server.

Possible values: ENABLED, DISABLED Default value: DISABLED

ssl3 State of SSLv3 protocol support for the SSL Virtual Server. Note: On platforms with SSL acceleration chips, if the SSL chip does not support SSLv3, this parameter cannot be set to ENABLED.

Possible values: ENABLED, DISABLED Default value: ENABLED

tls1 State of TLSv1.0 protocol support for the SSL Virtual Server.

Possible values: ENABLED, DISABLED Default value: ENABLED

tls11 State of TLSv1.1 protocol support for the SSL Virtual Server.

Possible values: ENABLED, DISABLED Default value: ENABLED

tls12 State of TLSv1.2 protocol support for the SSL Virtual Server.

Possible values: ENABLED, DISABLED Default value: ENABLED

tls13 State of TLSv1.3 protocol support for the SSL Virtual Server.

Possible values: ENABLED, DISABLED Default value: DISABLED

dtls1 State of DTLSv1.0 protocol support for the SSL Virtual Server.

Possible values: ENABLED, DISABLED Default value: ENABLED

dtls12 State of DTLSv1.2 protocol support for the SSL Virtual Server.

Possible values: ENABLED, DISABLED Default value: DISABLED

SNIEnable State of the Server Name Indication (SNI) feature on the virtual server and service-based offload. SNI helps to enable SSL encryption on multiple domains on a single virtual server or service if the domains are controlled by the same organization and share the same second-level domain name. For example, *.sports.net can be used to secure domains such as login.sports.net and help.sports.net.

Possible values: ENABLED, DISABLED Default value: DISABLED

ocspStapling State of OCSP stapling support on the SSL virtual server. Supported only if the protocol used is higher than SSLv3. Possible values: ENABLED: The appliance sends a request to the OCSP responder to check the status of the server certificate and caches the response for the specified time. If the response is valid at the time of SSL handshake with the client, the OCSP-based server certificate status is sent to the client during the handshake. DISABLED: The appliance does not check the status of the server certificate.

Possible values: ENABLED, DISABLED Default value: DISABLED

pushEncTrigger Trigger encryption on the basis of the PUSH flag value. Available settings function as follows:

- ALWAYS - Any PUSH packet triggers encryption.

- IGNORE - Ignore PUSH packet for triggering encryption.
- MERGE - For a consecutive sequence of PUSH packets, the last PUSH packet triggers encryption.
- TIMER - PUSH packet triggering encryption is delayed by the time defined in the set ssl parameter command or in the Change Advanced SSL Settings dialog box.

Possible values: Always, Merge, Ignore, Timer

sendCloseNotify Enable sending SSL Close-Notify at the end of a transaction

Possible values: YES, NO Default value: YES

dtlsProfileName Name of the DTLS profile whose settings are to be applied to the virtual server.

sslProfile Name of the SSL profile that contains SSL settings for the virtual server.

HSTS State of HSTS protocol support for the SSL Virtual Server. Using HSTS, a server can enforce the use of an HTTPS connection for all communication with a client

Possible values: ENABLED, DISABLED Default value: DISABLED

maxage Set the maximum time, in seconds, in the strict transport security (STS) header during which the client must send only HTTPS requests to the server Default value: 0 Minimum value: 0 Maximum value: 4294967294

IncludeSubdomains Enable HSTS for subdomains. If set to Yes, a client must send only HTTPS requests for subdomains.

Possible values: YES, NO Default value: NO

preload Flag indicates the consent of the site owner to have their domain preloaded.

Possible values: YES, NO Default value: NO

strictSigDigestCheck Parameter indicating to check whether peer entity certificate during TLS1.2 handshake is signed with one of signature-hash combination supported by Citrix ADC.

Possible values: ENABLED, DISABLED Default value: DISABLED

zeroRttEarlyData State of TLS 1.3 0-RTT early data support for the SSL Virtual Server. This setting only has an effect if resumption is enabled, as early data cannot be sent along with an initial handshake. Early application data has significantly different security properties - in particular there is no guarantee that the data cannot be replayed.

Possible values: ENABLED, DISABLED Default value: DISABLED

tls13SessionTicketsPerAuthContext Number of tickets the SSL Virtual Server will issue anytime TLS 1.3 is negotiated, ticket-based resumption is enabled, and either (1) a handshake completes or (2) post-handhsake client auth completes. This value can be increased to enable clients to open multiple parallel connections using a fresh ticket for each connection. No tickets are sent if resumption is disabled. Default value: 1 Minimum value: 1 Maximum value: 10

dheKeyExchangeWithPsk Whether or not the SSL Virtual Server will require a DHE key exchange to occur when a PSK is accepted during a TLS 1.3 resumption handshake. A DHE key exchange ensures forward secrecy even in the event that ticket keys are compromised, at the expense of an additional round trip and resources required to carry out the DHE key exchange. If disabled, a DHE key exchange will be performed when a PSK is accepted but only if requested by the client. If enabled, the server will require a DHE key exchange when a PSK is accepted regardless of whether the client supports combined PSK-DHE key exchange. This setting only has an effect when resumption is enabled.

Possible values: YES, NO Default value: NO

Example

1)set ssl vserver sslvip -dh ENABLED -dhFile /siteA/dh1024.pem -dhCount 500 The above example set the DH parameters for the SSL virtual server 'sslvip'. 3)set ssl vserver sslvip -ssl2 DISABLED The above example disables the support for SSLv2 protocol for the SSL virtual server 'sslvip'.

bind ssl vserver

Binds an SSL certificate-key pair or SSL certificate-key bundle or an SSL policy to an SSL virtual server.

Synopsis

bind ssl vserver <vServerName>@ ((-policyName <string>) | ((-certkeyName <string> [(-CA) | -SNICert]) | ((-certkeyBundleName <string>) | -cipherName <string> | -eccCurveName <eccCurveName>)))

Arguments

vServerName Name of the SSL virtual server.

policyName Name of the SSL policy to bind to the SSL virtual server.

priority Integer specifying the policy's priority. The lower the number, the higher the priority. Minimum value: 0 Maximum value: 64000

gotoPriorityExpression Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label. Default value: "END"

invoke Invoke policies bound to a virtual server, service, or user-defined policy label. After the invoked policies are evaluated, the flow returns to the policy with the next priority.

labelType Type of policy label to invoke.

Possible values: vserver, service, policylabel

labelName Name of the policy label, virtual server, or service to invoke if the current policy rule evaluates to TRUE.

type Bind point to which to bind the policy. Possible Values: REQUEST, INTERCEPT_REQ and CLIENTHELLO_REQ. These bindpoints mean:

1. REQUEST: Policy evaluation will be done at appplication above SSL. This bindpoint is default and is used for actions based on clientauth and client cert.
2. INTERCEPT_REQ: Policy evaluation will be done during SSL handshake to decide whether to intercept or not. Actions allowed with this type are: INTERCEPT, BYPASS and RESET.
3. CLIENTHELLO_REQ: Policy evaluation will be done during handling of Client Hello Request. Action allowed with this type is: RESET, FORWARD and PICKCACERTGRP.

Possible values: INTERCEPT_REQ, REQUEST, CLIENTHELLO_REQ Default value: REQUEST

certkeyName Name of the certificate-key pair.

CA Name of the CA certificate that issues and signs the intermediate-CA certificate or the end-user client or server certificate.

crlCheck Rule to use for the CRL corresponding to the CA certificate during client authentication. Available settings function as follows:

- MANDATORY - Deny SSL clients if the CRL is missing or expired, or the Next Update date is in the past, or the CRL is incomplete.
- OPTIONAL - Allow SSL clients if the CRL is missing or expired, or the Next Update date is in the past, or the CRL is incomplete, but deny if the client certificate is revoked in the CRL.

Possible values: Mandatory, Optional Default value: CRLCHECK_OPTIONAL

skipCAName The flag is used to indicate whether this particular CA certificates CA Name needs to be sent to the SSL client while requesting for client certificate in a SSL handshake

SNICert Name of the certificate-key pair to bind for use in SNI processing.

ocspCheck Rule to use for the OCSP responder associated with the CA certificate during client authentication. If MANDATORY is specified, deny all SSL clients if the OCSP check fails because of connectivity issues with the remote OCSP server, or any other reason that prevents the OCSP check. With the OPTIONAL setting, allow SSL clients even if the OCSP check fails except when the client certificate is revoked.

Possible values: Mandatory, Optional

certkeyBundleName Name of the certificate-key bundle.

SNICertkeybundle Use this option to bind certkeybundle which will be used in SNI processing.

cipherName Name of the individual cipher, user-defined cipher group, or predefined (built-in) cipher alias.

eccCurveName Named ECC curve bound to service/vserver.

Possible values: ALL, P_224, P_256, P_384, P_521

Example

1. bind ssl vserver ssl_vip -certkeyName cert1 In the above example the certificate cert1 is bound to the SSL vserver ssl_vip as server certificate.
2. bind ssl vserver ssl_vip -certkeyName cert2 -CA In the above example the certificate cert2 is bound to the SSL vserver ssl_vip as CA certificate.
3. bind ssl vserver ssl_vip -certkeyName cert3 -CA -ocspCheck Mandatory In the above example the certificate cert3 is bound to the SSL vserver ssl_vip as CA certificate, with OCSP check set to Mandatory.
4. bind ssl vserver ssl_vip -policyName certInsert_pol -priority 10 In the above example the SSL policy certInsert_pol is bound to the SSL vserver ssl_vip with priority 10.
5. bind ssl vserver ssl_vip -certkeyBundleName bundle1 In the above example the certificate bundle bundle1 is bound to the SSL vserver ssl_vip.

unbind ssl vserver

Unbinds an SSL policy, cipher, certificate-key pair and certificate-key bundle from an SSL virtual server.

Synopsis

unbind ssl vserver <vServerName>@ ((-policyName <string>) | ((-certkeyName <string>) | ((-certkeyBundleName <string>) | -cipherName <string> | -eccCurveName <eccCurveName>)))

Arguments

vServerName Name of the SSL virtual server.

policyName Name of the SSL policy to unbind from the SSL virtual server.

priority Priority of the NOPOLICY (built-in policy) to be unbound. Not required if you are unbinding a user-defined policy. Minimum value: 1 Maximum value: 2147483647

type Bind point to which to bind the policy. Possible Values: REQUEST, INTERCEPT_REQ and CLIENTHELLO_REQ. These bindpoints mean:

1. REQUEST: Policy evaluation will be done at appplication above SSL. This bindpoint is default and is used for actions based on clientauth and client cert.
2. INTERCEPT_REQ: Policy evaluation will be done during SSL handshake to decide whether to intercept or not. Actions allowed with this type are: INTERCEPT, BYPASS and RESET.
3. CLIENTHELLO_REQ: Policy evaluation will be done during handling of Client Hello Request. Action allowed with this type is: RESET, FORWARD and PICKCACERTGRP.

Possible values: INTERCEPT_REQ, REQUEST, CLIENTHELLO_REQ Default value: REQUEST

certkeyName The name of the certificate key pair binding.

CA CA certificate.

SNICert Name of the SNI certificate-key pair.

certkeyBundleName Certkeybundle name bound to the vserver.

SNICertkeybundle Use this option to bind certkeybundle which will be used in SNI processing.

cipherName Name of the cipher.

eccCurveName Named ECC curve bound to service/vserver.

Possible values: ALL, P_224, P_256, P_384, P_521

Example

unbind ssl vserver ssl_vip -policyName certInsert_pol

show ssl vserver

Displays SSL specific configuration information for all SSL virtual servers, or displays detailed information for the specified SSL virtual server.

Synopsis

show ssl vserver

Arguments

vServerName Name of the SSL virtual server for which to show detailed information.

Output

clearTextPort The clearTextPort settings.

dh The state of Diffie-Hellman (DH) key exchange support.

dhFile The file name and path for the DH parameter.

dhCount The refresh count for the re-generation of DH public-key and private-key from the DH parameter.

dhKeyExpSizeLimit This option enables the use of NIST recommended (NIST Special Publication 800-56A) bit size for private-key size. For example, for DH params of size 2048bit, the private-key size recommended is 224bits. This is rounded-up to 256bits.

eRSA The state of Ephemeral RSA key exchange support.Ephemeral RSA is used for export ciphers

eRSACount The refresh count for the re-generation of RSA public-key and private-key pair.

sessReuse The state of session re-use support.

sessTimeout The Session timeout value in seconds.

cipherRedirect The state of Cipher Redirect feature.Cipher Redirect feature can be used to provide more readable information to SSL clients about mismatch in ciphers between the client and the SSL vserver.

crlCheck The state of the CRL check parameter. (Mandatory/Optional)

cipherURL The redirect URL to be used with the Cipher Redirect feature.

sslv2Redirect The state of SSLv2 Redirect feature. SSLv2 Redirect feature can be used to provide more readable information to SSL client about non-support of SSLv2 protocol on the SSL vserver.

sslv2URL The redirect URL to be used with SSLv2 Redirect feature.

clientAuth The state of Client-Authentication support.

clientCert The rule for client certificate requirement in client authentication.

sslRedirect The state of HTTPS redirect feature support.

priority The priority of the policies bound to this SSL service

type Bind point to which to bind the policy. Possible Values: REQUEST, INTERCEPT_REQ and CLIENTHELLO_REQ. These bindpoints mean:

1. REQUEST: Policy evaluation will be done at appplication above SSL. This bindpoint is default and is used for actions based on clientauth and client cert.
2. INTERCEPT_REQ: Policy evaluation will be done during SSL handshake to decide whether to intercept or not. Actions allowed with this type are: INTERCEPT, BYPASS and RESET.
3. CLIENTHELLO_REQ: Policy evaluation will be done during handling of Client Hello Request. Action allowed with this type is: RESET, FORWARD and PICKCACERTGRP.

polinherit Whether the bound policy is a inherited policy or not

redirectPortRewrite The state of port rewrite feature support.

nonFipsCiphers The state of usage of non FIPS approved ciphers.

ssl2 The state of SSLv2 protocol support.

ssl3 The state of SSLv3 protocol support.

tls1 The state of TLSv1.0 protocol support.

tls11 The state of TLSv1.1 protocol support.

tls12 The state of TLSv1.2 protocol support.

tls13 The state of TLSv1.3 protocol support.

dtls1 The state of DTLSv1.0 protocol support.

dtls12 The state of DTLSv1.2 protocol support.

SNIEnable The state of SNI extension.Server Name Indication (SNI) helps to enable SSL encryption on multiple subdomains if the domains are controlled by the same organization and share the same second-level domain name. State of SNI feature on service

ocspStapling State of OCSP stapling support on the SSL virtual server. Supported only if the protocol used is higher than SSLv3. Possible values: ENABLED: The appliance sends a request to the OCSP responder to check the status of the server certificate and caches the response for the specified time. If the response is valid at the time of SSL handshake with the client, the OCSP-

based server certificate status is sent to the client during the handshake. DISABLED: The appliance does not check the status of the server certificate.

cipherAliasName/cipherName/cipherGroupName The name of the cipher group/alias/individual cipheri bindings.

cipherName The cipher group/alias/individual cipher configuration

description The cipher suite description.

service Service

certkeyName The name of the certificate key pair binding.

certkeyBundleName Certkeybundle name bound to the vserver.

policyName The name of the SSL policy binding.

invoke Invoke flag. This attribute is relevant only for ADVANCED policies

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

serviceName Service name.

ocspCheck The state of the OCSP check parameter. (Mandatory/Optional)

pushEncTrigger PUSH packet triggering encryption: Always, Ignore, Merge

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

CA CA certificate.

SNICert The name of the CertKey. Use this option to bind Certkey(s) which will be used in SNI processing.

SNICertkeybundle Use this option to bind certkeybundle which will be used in SNI processing.

eccCurveName Named ECC curve bound to vserver/service.

stateflag skipCAName The flag is used to indicate whether this particular CA certificate's CA_Name needs to be sent to the SSL client while requesting for client certificate in a SSL handshake

sendCloseNotify Enable sending SSL Close-Notify at the end of a transaction

dtlsProfileName Name of the DTLS profile whose settings are to be applied to the virtual server.

dtlsFlag The flag is used to indicate whether DTLS is set or not

quicFlag This flag is used to indicate the use of the QUIC transport protocol by an SSL virtual server or service.

sslProfile Name of the SSL profile that contains SSL settings for the virtual server.

HSTS State of HSTS protocol support for the SSL Virtual Server. Using HSTS, a server can enforce the use of an HTTPS connection for all communication with a client

maxage Set the maximum time, in seconds, in the strict transport security (STS) header during which the client must send only HTTPS requests to the server

IncludeSubdomains Enable HSTS for subdomains. If set to Yes, a client must send only HTTPS requests for subdomains.

preload Flag indicates the consent of the site owner to have their domain preloaded.

strictSigDigestCheck Parameter indicating to check whether peer entity certificate during TLS1.2 handshake is signed with one of signature-hash combination supported by Citrix ADC.

zeroRttEarlyData State of TLS 1.3 0-RTT early data support for the SSL Virtual Server. This setting only has an effect if resumption is enabled, as early data cannot be sent along with an initial handshake. Early application data has significantly different security properties - in particular there is no guarantee that the data cannot be replayed.

tls13SessionTicketsPerAuthContext Number of tickets the SSL Virtual Server will issue anytime TLS 1.3 is negotiated, ticket-based resumption is enabled, and either (1) a handshake completes or (2) post-handhsake client auth completes. This value can be increased to enable clients to open multiple parallel connections using a fresh ticket for each connection. No tickets are sent if resumption is disabled.

dheKeyExchangeWithPsk Whether or not the SSL Virtual Server will require a DHE key exchange to occur when a PSK is accepted during a TLS 1.3 resumption handshake. A DHE key exchange ensures forward secrecy even in the event that ticket keys are compromised, at the expense of an additional round trip and resources required to carry out the DHE key exchange. If disabled, a DHE key exchange will be performed when a PSK is accepted but only if requested by the client. If enabled, the server will require a DHE key exchange when a PSK is accepted

regardless of whether the client supports combined PSK-DHE key exchange. This setting only has an effect when resumption is enabled.

devno count

Example

An example of the output of the show vserver sslvip command is as follows: sh ssl vserver va1

```
    Advanced SSL configuration for VServer va1:

    DH: DISABLED

    Ephemeral RSA: ENABLED          Refresh Count: 0

    Session Reuse: ENABLED          Timeout: 120 seconds

    Cipher Redirect: DISABLED

    SSLv2 Redirect: DISABLED

    ClearText Port: 0

    Client Auth: DISABLED

    SSL Redirect: DISABLED

    Non FIPS Ciphers: DISABLED

    SSLv2: DISABLED SSLv3: ENABLED  TLSv1: ENABLED



    1 bound certificate:
```

1. ```
   CertKey Name: buy       Server Certificate



   1 bound CA certificate:
   ```
   ```

2.
```
CertKey Name: rtca      CA Certificate



1)      Cipher Name: DEFAULT

Description: Predefined Cipher Alias
```

Related Commands

- bind ssl cipher

stat ssl vserver

Displays statistics for all SSL virtual servers, or displays detailed statistics for the specified SSL virtual server.

Synopsis

stat ssl vserver

Arguments

vServerName Name of the SSL virtual server for which to show detailed statistics

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Vserver Health (Health) Health of the vserver. This gives percentage of UP services bound to this vserver.

Vserver IP address (vsvrIP) IP address of the vserver

Port (port) The port on which the service is running.

Vserver protocol (Protocol) Protocol associated with the vserver

State Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)

total ACTIVE services (actSvcs) number of ACTIVE services bound to a vserver

Client Authentication Success (sslTotClientAuthSuccess) Number of successful client authentication on this vserver

Client Authentication Failure (sslTotClientAuthFailure) Number of failure client authentication on this vserver

Total encrypted bytes (sslCtxTotEncBytes) Number of encrypted bytes per SSL vserver

Total decrypted bytes (sslCtxTotDecBytes) Number of decrypted bytes per SSL vserver

Total hardware encrypted bytes (sslCtxTotHwEncBytes) Number of hardware encrypted bytes per SSL vserver

Total hardware decrypted bytes (sslCtxTotHwDec_Bytes) Number of hw decrypted bytes per SSL vserver

Total new sessions created (sslCtxTotSessionNew) Number of new sessions created

Total session hits (sslCtxTotSessionHits) Number of session hits

ssl-wrapkey

The following operations can be performed on "ssl-wrapkey":

rm| create| show|

rm ssl wrapkey

Removes all the wrap keys, or the specified wrap key, from the appliance.

Synopsis

rm ssl wrapkey <wrapKeyName> ...

Arguments

wrapKeyName Name of the wrap key to remove.

Example

rm wrapkey wrap1

create ssl wrapkey

Generates a wrap key.

Synopsis

create ssl wrapkey <wrapKeyName> {-password } {-salt }

Arguments

wrapKeyName Name for the wrap key. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the wrap key is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my key" or 'my key').

password Password string for the wrap key.

salt Salt string for the wrap key.

Example

create wrapkey wrap1 -password wrapkey123 -salt wrapsalt123

show ssl wrapkey

Display the wrap keys.

Synopsis

show ssl wrapkey

Arguments

Output

wrapKeyName Wrap key name.

devno count stateflag

Example

An example of output of 'show wrapkey' command is as shown below: sh wrapkey 1 WRAP key: 1)WRAP Key Name: wrap1

ssl

The following operations can be performed on "ssl":

stat ssl

Displays SSL statistics.

Synopsis

stat ssl

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Bytes decrypted on the back-end (secondary card) (DecHwBeSecondary) Number of bytes decrypted on the back-end in hardware on secondary card.

Bytes decrypted on the front-end (secondary card) (DecHwFeSecondary) Number of bytes decrypted on the front-end in hardware on secondary card.

Bytes encrypted on the back-end (secondary card) (EncHwBeSecondary) Number of bytes encrypted on the back-end in hardware on secondary card.

Bytes encrypted on the front-end (secondary card) (EncHwFeSecondary) Number of bytes encrypted on the front-end in hardware on secondary card.

ECDSA_P521 (SSLECDSAP521CryptoUtilStat) Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

ECDSA_P384 (SSLECDSAP384CryptoUtilStat) Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

ECDSA_P256 (SSLECDSAP256CryptoUtilStat) Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

ECDSA_P224 (SSLECDSAP224CryptoUtilStat) Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

ECDSA Crypto Utilization (SSLAsymECDSACryptoUtilStat) Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

ECDH_P521 (SSLECDHP521CryptoUtilStat) Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

ECDH_P384 (SSLECDHP384CryptoUtilStat) Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

ECDH_P256 (SSLECDHP256CryptoUtilStat) Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

ECDH_P224 (SSLECDHP224CryptoUtilStat) Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

ECDH Crypto Utilization (SSLAsymECDHCryptoUtilStat) Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

DH Crypto Utilization (SSLAsymDHCryptoUtilStat) Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

RSA_Others (SSLAsymRSAOthersCryptoUtilStat) Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

RSA_1K (SSLAsymRSA1KCryptoUtilStat) Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

RSA_2K (SSLAsymRSA2KCryptoUtilStat) Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

RSA_4K (SSLAsymRSA4KCryptoUtilStat) Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

RSA Crypto Utilization (SSLAsymRSACryptoUtilStat) Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

Bytes decrypted (secondary card) (DecHwSecondary) Number of bytes decrypted in hardware on secondary card.

Bytes encrypted (secondary card) (EncHwSecondary) Number of bytes encrypted in hardware on secondary card.

Symmetric Crypto Utilization (SSLSymCryptoUtilStat) Utilization of the hardware symmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

Asymmetric Crypto Utilization (SSLAsymCryptoUtilStat) Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

SSL Crypto Utilization Symm (%) (SSLCryptoUtilSymmStat) Utilization of the hardware symmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

SSL Crypto Utilization Asym (%) (SSLCryptoUtilAsymStat) Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

Secondary card utilization (%) (SSLCryptoUtilStat2nd) Utilization of the hardware crypto resource. Only valid values are 0-100%. Only works on N3FIPS+N3 hybrid platform.

SSL crypto utilization (%) (SSLCryptoUtilStat) Utilization of the hardware crypto resource. Only valid values are 0-100%. Only works on platforms with Nitrox-3 chips.

 # Secondary SSL cards UP (SSLCardUPSecondary) Number of Add on SSL cards that are UP.

 # Secondary SSL cards present (SSLCardsSecondary) Number of secondary SSL crypto cards present on the Citrix ADC.

SSL crypto card status (SSLCardSt) Status of the SSL card(s). The value should be interpreted in binary form, with each set bit indicates a card as UP.

 # ssl cards present (SSLCards) Number of SSL crypto cards present on the Citrix ADC.

 # ssl cards UP (SSLCardUP) Number of SSL cards that are UP. If the number of cards UP is lower than a threshold, a failover is initiated.

SSL engine status (SSLEngSt) State of the SSL Engine (1=UP/0=DOWN). This state is decided based on SSL Feature/License status and minimum number of cards UP.

SSL sessions (SSLSe) Number of SSL sessions on the Citrix ADC.

SSL transactions (SSLTrn) Number of SSL transactions on the Citrix ADC

SSLv2 transactions (SSL2Trn) Number of SSLv2 transactions on the Citrix ADC.

SSLv3 transactions (SSL3Trn) Total number of SSLv3 transactions on the Citrix ADC.

TLSv1 transactions (TLS1Trn) Number of TLSv1 transactions on the Citrix ADC.

TLSv1.1 transactions (TLS11Trn) Number of TLSv1.1 transactions on the Citrix ADC.

TLSv1.2 transactions (TLS12Trn) Number of TLSv1.2 transactions on the Citrix ADC.

TLSv1.3 transactions (TLS13Trn) Number of TLSv1.3 transactions on the Citrix ADC.

DTLSv1 transactions (DTLS1Trn) Number of DTLSv1 transactions on the Citrix ADC.

DTLSv1.2 transactions (DTLS12Trn) Number of DTLSv1.2 transactions on the Citrix ADC.

SSLv2 sessions (SSL2Se) Number of SSLv2 sessions on the Citrix ADC.

SSLv3 sessions (SSL3Se) Number of SSLv3 sessions on the Citrix ADC.

TLSv1 sessions (TLS1Se) Number of TLSv1 sessions on the Citrix ADC.

TLSv1.1 sessions (TLS11Se) Number of TLSv1.1 sessions on the Citrix ADC.

TLSv1.2 sessions (TLS12Se) Number of TLSv1.2 sessions on the Citrix ADC.

TLSv1.3 sessions (TLS13Se) Number of TLSv1.3 sessions on the Citrix ADC.

DTLSv1 sessions (DTLS1Se) Number of DTLSv1 sessions on the Citrix ADC.

DTLSv1.2 sessions (DTLS12Se) Number of DTLSv1.2 sessions on the Citrix ADC.

new SSL sessions (NewSe) Number of new SSL sessions created on the Citrix ADC.

SSL session misses (SeMiss) Number of SSL session reuse misses on the Citrix ADC.

SSL session hits (SeHit) Number of SSL session reuse hits on the Citrix ADC.

SSL sessions (BSSLSe) Number of back-end SSL sessions on the Citrix ADC.

SSLv3 sessions (BSSL3Se) Number of back-end SSLv3 sessions on the Citrix ADC.

TLSv1 sessions (BTLS1Se) Number of back-end TLSv1 sessions on the Citrix ADC.

TLSv1.1 sessions (BTLS1Se) Number of back-end TLSv1.1 sessions on the Citrix ADC.

TLSv1.2 sessions (BTLS1Se) Number of back-end TLSv1.2 sessions on the Citrix ADC.

DTLSv1 sessions (BDTLS1Se) Number of back-end DTLSv1 sessions on the Citrix ADC.

Session multiplex attempts (BSeMx) Number of back-end SSL session multiplex attempts on the Citrix ADC.

Session multiplex successes (BSeMxS) Number of back-end SSL session multiplex successes on the Citrix ADC.

Session multiplex failures (BSeMxF) Number of back-end SSL session multiplex failures on the Citrix ADC.

Bytes encrypted (Enc) Number of bytes encrypted on the Citrix ADC.

Bytes decrypted (Dec) Number of bytes decrypted on the Citrix ADC.

Server in record (ServerInRecord) Number server in record on the Citrix ADC.

SSL session renegotiations (SSLRn) Number of SSL session renegotiations on the Citrix ADC.

SSLv3 session renegotiations (SSL3Rn) Number of session renegotiations done on SSLv3.

TLSv1 session renegotiations (TLS1Rn) Number of SSL session renegotiations done on TLSv1.

TLSv1.1 session renegotiations (TLS11Rn) Number of SSL session renegotiations done on TLSv1.1.

TLSv1.2 session renegotiations (TLS12Rn) Number of SSL session renegotiations done on TLSv1.2.

DTLSv1 session renegotiations (DTLS1Rn) Number of SSL session renegotiations done on DTLSv1.

DTLSv1.2 session renegotiations (DTLS12Rn) Number of SSL session renegotiations done on DTLSv1.2.

RSA 512-bit key exchanges (RSAKx5) Number of RSA 512-bit key exchanges on the Citrix ADC.

RSA 1024-bit key exchanges (RSAKx1) Number of RSA 1024-bit key exchanges on the Citrix ADC.

RSA 2048-bit key exchanges (RSAKx2) Number of RSA 2048-bit key exchanges on the Citrix ADC.

RSA 3072-bit key exchanges (RSAKx3) Number of RSA 3072-bit key exchanges on the Citrix ADC.

RSA 4096-bit key exchanges (RSAKx4) Number of RSA 4096-bit key exchanges on the Citrix ADC.

DH 512-bit key exchanges (DHKx5) Number of Diffie-Helman 512-bit key exchanges on the Citrix ADC.

DH 1024-bit key exchanges (DHKx1) Number of Diffie-Helman 1024-bit key exchanges on the Citrix ADC.

DH 2048-bit key exchanges (DHKx2) Number of Diffie-Helman 2048-bit key exchanges on the Citrix ADC.

DH 4096-bit key exchanges (DHKx4) Number of Diffie-Helman 4096-bit key exchanges on the Citrix ADC.

ECDHE 521 curve key exchanges (ECDHEKx521) Number of 521 Elliptical Curve Diffie-Helman on the Citrix ADC.

ECDHE 384 curve key exchanges (ECDHEKx384) Number of 384 Elliptical Curve Diffie-Helman on the Citrix ADC.

ECDHE 256 curve key exchanges (ECDHEKx256) Number of 256 Elliptical Curve Diffie-Helman on the Citrix ADC.

ECDHE 224 curve key exchanges (ECDHEKx224) Number of 224 Elliptical Curve Diffie-Helman on the Citrix ADC.

Total ECDHE key exchanges (ECDHEKx) Total ECDHE Transactions on Citrix ADC.

RC4 40-bit encryptions (RC4En4) Number of RC4 40-bit cipher encryptions on the Citrix ADC.

RC4 56-bit encryptions (RC4En5) Number of RC4 56-bit cipher encryptions on the Citrix ADC.

RC4 64-bit encryptions (RC4En6) Number of RC4 64-bit cipher encryptions on the Citrix ADC.

RC4 128-bit encryptions (RC4En1) Number of RC4 128-bit cipher encryptions on the Citrix ADC.

DES 40-bit encryptions (DESEn4) Number of DES 40-bit cipher encryptions on the Citrix ADC.

DES 56-bit encryptions (DESEn5) Number of DES 56-bit cipher encryptions on the Citrix ADC.

3DES 168-bit encryptions (3DESEn1) Number of DES 168-bit cipher encryptions on the Citrix ADC.

AES 128-bit encryptions (AESEn1) Number of AES 128-bit cipher encryptions on the Citrix ADC.

AES 256-bit encryptions (AESEn2) Number of AES 256-bit cipher encryptions on the Citrix ADC.

RC2 40-bit encryptions (RC2En4) Number of RC2 40-bit cipher encryptions on the Citrix ADC.

RC2 56-bit encryptions (RC2En5) Number of RC2 56-bit cipher encryptions on the Citrix ADC.

RC2 128-bit encryptions (RC2En1) Number of RC2 128-bit cipher encryptions on the Citrix ADC.

AES-GCM 128-bit encryptions (AESGCMEn1) Number of AEC-GCM 128-bit cipher encryptions on the Citrix ADC.

AES-GCM 256-bit encryptions (AESGCMEn2) Number of AEC-GCM 256-bit cipher encryptions on the Citrix ADC.

Null cipher encryptions (NullEn) Number of Null cipher encryptions on the Citrix ADC.

MD5 hashes (MD5Hsh) Number of MD5 hashes on the Citrix ADC.

SHA hashes (SHAHsh) Number of SHA hashes on the Citrix ADC.

SHA256 hashes (SHA256Hsh) Number of SHA256 hashes on the Citrix ADC.

SHA384 hashes (SHA384Hsh) Number of SHA384 hashes on the Citrix ADC.

SSLv2 SSL handshakes (SSL2Hs) Number of handshakes on SSLv2 on the Citrix ADC.

SSLv3 SSL handshakes (SSL3Hs) Number of handshakes on SSLv3 on the Citrix ADC.

TLSv1 SSL handshakes (TLS1Hs) Number of SSL handshakes on TLSv1 on the Citrix ADC.

TLSv1.1 SSL handshakes (TLS11Hs) Number of SSL handshakes on TLSv1.1 on the Citrix ADC.

TLSv1.2 SSL handshakes (TLS12Hs) Number of SSL handshakes on TLSv1.2 on the Citrix ADC.

TLSv1.3 SSL handshakes (TLS13Hs) Number of SSL handshakes on TLSv1.3 on the Citrix ADC.

DTLSv1 SSL handshakes (DTLS1Hs) Number of SSL handshakes on DTLSv1 on the Citrix ADC.

DTLSv1.2 SSL handshakes (DTLS12Hs) Number of SSL handshakes on DTLSv1.2 on the Citrix ADC.

SSLv2 client authentications (SSL2CAt) Number of client authentications done on SSLv2.

SSLv3 client authentications (SSL3CAt) Number of client authentications done on SSLv3.

TLSv1 client authentications (TLS1CAt) Number of client authentications done on TLSv1.

TLSv1.1 client authentications (TLS11CAt) Number of client authentications done on TLSv1.1.

TLSv1.2 client authentications (TLS12CAt) Number of client authentications done on TLSv1.2.

TLSv1.3 client authentications (TLS13CAt) Number of client authentications done on TLSv1.3.

DTLSv1 client authentications (DTLS1CAt) Number of client authentications done on DTLSv1.

DTLSv1.2 client authentications (DTLS12CAt) Number of client authentications done on DTLSv1.2.

RSA authentications (RSAAt) Number of RSA authentications on the Citrix ADC.

DH authentications (DHAt) Number of Diffie-Helman authentications on the Citrix ADC.

DSS (DSA) authentications (DSSAt) Total number of times DSS authorization is used on the Citrix ADC.

ECDSA authentications (ECDSAAt) Total number of times ECDSA authorization is used on the Citrix ADC.

Null authentications (NullAt) Number of Null authentications on the Citrix ADC.

SSL session renegotiations (BSSLRn) Number of back-end SSL session renegotiations on the Citrix ADC.

SSLv3 session renegotiations (BSSL3Rn) Number of back-end SSLv3 session renegotiations on the Citrix ADC.

TLSv1 session renegotiations (BTLS1Rn) Number of back-end TLSv1 session renegotiations on the Citrix ADC.

TLSv1.1 back-end session renegotiations (BTLS1aRn) Number of back-end TLSv1.1 session renegotiations on the Citrix ADC.

TLSv1.2 back-end session renegotiations (BTLS12Rn) Number of back-end TLSv1.2 session renegotiations on the Citrix ADC.

DTLSv1 session renegotiations (BDTLS1Rn) Number of back-end DTLSv1 session renegotiations on the Citrix ADC.

RSA 512-bit key exchanges (BRSAKx5) Number of back-end RSA 512-bit key exchanges on the Citrix ADC.

RSA 1024-bit key exchanges (BRSAKx1) Number of back-end RSA 1024-bit key exchanges on the Citrix ADC.

RSA 2048-bit key exchanges (BRSAKx2) Number of back-end RSA 2048-bit key exchanges on the Citrix ADC.

RSA 3072-bit key exchanges (BRSAKx3) Number of back-end RSA 3072-bit key exchanges on the Citrix ADC.

RSA 4096-bit key exchanges (BRSAKx4) Number of back-end RSA 4096-bit key exchanges on the Citrix ADC.

DH 512-bit key exchanges (BDHKx5) Number of back-end DH 512-bit key exchanges on the Citrix ADC.

DH 1024-bit key exchanges (BDHKx1) Number of back-end DH 1024-bit key exchanges on the Citrix ADC.

DH 2048-bit key exchanges (BDHKx2) Number of back-end DH 2048-bit key exchanges on the Citrix ADC.

DH 4096-bit key exchanges (BDHKx4) Number of back-end DH 4096-bit key exchanges on the Citrix ADC.

ECDHE 521 curve key exchanges (BECDHECx1) Number of back-end ECDHE 521 curve Key exchanges on the Citrix ADC.

ECDHE 384 curve key exchanges (BECDHECx2) Number of back-end ECDHE 384 curve Key exchanges on the Citrix ADC.

ECDHE 256 curve key exchanges (BECDHECx3) Number of back-end ECDHE 256 curve Key exchanges on the Citrix ADC.

ECDHE 224 curve key exchanges (BECDHECx4) Number of back-end ECDHE 224 curve Key exchanges on the Citrix ADC.

RC4 40-bit encryptions (BRC4En4) Number of back-end RC4 40-bit cipher encryptions on the Citrix ADC.

RC4 56-bit encryptions (BRC4En5) Number of back-end RC4 56-bit cipher encryptions on the Citrix ADC.

RC4 64-bit encryptions (BRC4En6) Number of back-end RC4 64-bit cipher encryptions on the Citrix ADC.

RC4 128-bit encryptions (BRC4En1) Number of back-end RC4 128-bit cipher encryptions on the Citrix ADC.

DES 40-bit encryptions (BDESEn4) Number of back-end DES 40-bit cipher encryptions on the Citrix ADC.

DES 56-bit encryptions (BDESEn5) Number of back-end DES 56-bit cipher encryptions on the Citrix ADC.

3DES 168-bit encryptions (B3DESE1n) Number of back-end 3DES 168-bit cipher encryptions on the Citrix ADC.

AES 128-bit encryptions (BAESEn1) Back-end AES 128-bit cipher encryptions on the Citrix ADC.

AES 256-bit encryptions (BAESEn2) Back-end AES 256-bit cipher encryptions on the Citrix ADC.

RC2 40-bit encryptions (BRC2En4) Number of back-end RC2 40-bit cipher encryptions on the Citrix ADC.

RC2 56-bit encryptions (BRC2En5) Number of back-end RC2 56-bit cipher encryptions on the Citrix ADC.

RC2 128-bit encryptions (BRC2En1) Number of back-end RC2 128-bit cipher encryptions on the Citrix ADC.

AES-GCM 128-bit encryptions (BAESGCMEn1) Back-end AES-GCM 128-bit cipher encryptions on the Citrix ADC.

AES-GCM 256-bit encryptions (BAESGCMEn2) Back-end AES-GCM 256-bit cipher encryptions on the Citrix ADC .

null encryptions (BNullEn) Number of back-end null cipher encryptions on the Citrix ADC.

MD5 hashes (BMD5Hsh) Number of back-end MD5 hashes on the Citrix ADC.

SHA hashes (BSHAHsh) Number of back-end SHA hashes on the Citrix ADC.

SHA256 hashes (BSHA256Hsh) Number of back-end SHA256 hashes on the Citrix ADC.

SHA384 hashes (BSHA384Hsh) Number of back-end SHA384 hashes on the Citrix ADC.

SSLv3 handshakes (BSSL3Hs) Number of back-end SSLv3 handshakes on the Citrix ADC.

TLSv1 handshakes (BTLS1Hs) Number of back-end TLSv1 handshakes on the Citrix ADC.

TLSv1.1 handshakes (BTLS11Hs) Number of back-end TLSv1.1 handshakes on the Citrix ADC.

TLSv1.2 handshakes (BTLS12Hs) Number of back-end TLSv1.2 handshakes on the Citrix ADC.

DTLSv1 handshakes (BDTLS1Hs) Number of back-end DTLSv1 handshakes on the Citrix ADC.

SSLv3 client authentications (BSSL3CAt) Number of back-end SSLv3 client authentications on the Citrix ADC.

TLSv1 client authentications (BTLS1CAt) Number of back-end TLSv1 client authentications on the Citrix ADC.

TLSv1.1 client authentications (BTLS11CAt) Number of back-end TLSv1.1 client authentications on the Citrix ADC.

TLSv1.2 client authentications (BTLS12CAt) Number of back-end TLSv1.2 client authentications on the Citrix ADC.

DTLSv1 client authentications (BDTLS1CAt) Number of back-end DTLSv1 client authentications on the Citrix ADC.

RSA authentications (BRSAAt) Number of back-end RSA authentications on the Citrix ADC.

DH authentications (BDHAt) Number of back-end DH authentications on the Citrix ADC.

DSS authentications (BDSSAt) Number of back-end DSS authentications on the Citrix ADC.

ECDSA authentications (BECDSAAt) Number of back-end ECDSA authentications on the Citrix ADC.

Null authentications (BNullAt) Number of back-end null authentications on the Citrix ADC.

RSA key exchanges offloaded (RSAkxOf) Number of RSA key exchanges offloaded to the cryptography card.

RSA sign operations offloaded (RSASnOf) Number of RSA sign operations offloaded to the cryptography card.

DH key exchanges offloaded (DHkxOf) Number of DH key exchanges offloaded to the cryptography card.

RC4 encryptions offloaded (RC4EnOf) Number of RC4 encryptions offloaded to the cryptography card.

DES encryptions offloaded (DESEnOf) Number of DES encryptions offloaded to the cryptography card.

AES encryptions offloaded (AESEnOf) Number of AES encryptions offloaded to the cryptography card.

AES-GCM 128-bit encryptions offloaded (AESGCMEnOf1) Number of AES-GCM 128-bit encryptions offloaded to the cryptography card.

AES-GCM 256-bit encryptions offloaded (AESGCMEnOf2) Number of AES-GCM 256-bit encryptions offloaded to the cryptography card.

Bytes encrypted in hardware (EncHw) Number of bytes encrypted in hardware.

Bytes encrypted in software (EncSw) Number of bytes encrypted in software.

Bytes encrypted on the front-end. (EncFe) Number of bytes encrypted on the front-end.

Bytes encrypted in hardware on the front-end. (EncHwFe) Number of bytes encrypted in hardware on the front-end.

Bytes encrypted in software on the front-end (EncSwFe) Number of bytes encrypted in software on the front-end.

Bytes encrypted on the back-end (EncBe) Number of bytes encrypted on the back-end.

Bytes encrypted in hardware on the back-end (EncHwBe) Number of bytes encrypted in hardware on the back-end.

Bytes encrypted in software on the back-end (EncSwBe) Number of bytes encrypted in software on the back-end.

Bytes decrypted in hardware (DecHw) Number of bytes decrypted in hardware.

Bytes decrypted in software (DecSw) Number of bytes decrypted in software.

Bytes decrypted on the front-end (DecFe) Number of bytes decrypted on the front-end.

Bytes decrypted in hardware on the front-end (DecHwFe) Number of bytes decrypted in hardware on the front-end.

Bytes decrypted in software on the front-end (DecSwFe) Number of bytes decrypted in software on the front-end.

Bytes decrypted on the back-end (DecBe) Number of bytes decrypted on the back-end.

Bytes decrypted in hardware on the back-end (DecHwBe) Number of bytes decrypted in hardware on the back-end.

Bytes decrypted in software on the back-end. (DecSwBe) Number of bytes decrypted in software on the back-end

Total SPCB in use (SPCBInUseCount) Number of SPCB in use.

Active SSL sessions (sessionInUse) Number of active SSL sessions on the Citrix ADC.

Current queue size (curQsize) Current queue size

In Q count for current card (CardInQCount) Number of current SSL card InQ count.

In BulkQ count for current card (CardinBlkQ) Number of current SSL card In BulkQ count.

In KeyQ count for current card (CardinKeyQ) Number of current SSL card In KeyQ count.

Backend SSL sessions reused (BSeRe) Number of back-end SSL sessions reused on the Citrix ADC.

IDEA 128-bit encryptions (IDEAEn1) Number of IDEA 128-bit cipher encryptions on the Citrix ADC.

IDEA 128-bit encryptions (BIDEAEn1) Number of back-end IDEA 128-bit cipher encryptions on the Citrix ADC.

 # Secondary SSL cards present (SSLCardsSecondary) Number of secondary SSL crypto cards present on the Citrix ADC.

 # Secondary SSL cards UP (SSLCardUPSecondary) Number of Add on SSL cards that are UP.

Bytes encrypted (secondary card) (EncHwSecondary) Number of bytes encrypted in hardware on secondary card.

Bytes decrypted (secondary card) (DecHwSecondary) Number of bytes decrypted in hardware on secondary card.

Bytes encrypted on the front-end (secondary card) (EncHwFeSecondary) Number of bytes encrypted on the front-end in hardware on secondary card.

Bytes encrypted on the back-end (secondary card) (EncHwBeSecondary) Number of bytes encrypted on the back-end in hardware on secondary card.

Bytes decrypted on the front-end (secondary card) (DecHwFeSecondary) Number of bytes decrypted on the front-end in hardware on secondary card.

Bytes decrypted on the back-end (secondary card) (DecHwBeSecondary) Number of bytes decrypted on the back-end in hardware on secondary card.

Related Commands

- stat ssl vserver

stream

Stream

The entities on which you can perform NetScaler CLI operations:

- stream-identifier
- stream-selector
- stream-session

stream-identifier

The following operations can be performed on "stream-identifier":

set| unset| rm| show| add| stat|

set stream identifier

Modifies the specified parameters of a stream identifier. Parameters for which a default value is available revert to their default values.

Synopsis

set stream identifier <name>

Arguments

name The name of stream identifier.

selectorName Name of the selector to use with the stream identifier.

interval Number of minutes of data to use when calculating session statistics (number of requests, bandwidth, and response times). The interval is a moving window that keeps the most recently collected data. Older data is discarded at regular intervals. Default value: 1 Minimum value: 1

SampleCount Size of the sample from which to select a request for evaluation. The smaller the sample count, the more accurate is the statistical data. To evaluate all requests, set the sample

count to 1. However, such a low setting can result in excessive consumption of memory and processing resources. Default value: 1 Minimum value: 1 Maximum value: 65535

sort Sort stored records by the specified statistics column, in descending order. Performed during data collection, the sorting enables real-time data evaluation through Citrix ADC policies (for example, compression and caching policies) that use functions such as IS_TOP(n).

Possible values: REQUESTS, CONNECTIONS, RESPTIME, BANDWIDTH, RESPTIME_BREACHES, NONE Default value: REQUESTS

snmptrap Enable/disable SNMP trap for stream identifier

Possible values: ENABLED, DISABLED Default value: DISABLED

appflowLog Enable/disable Appflow logging for stream identifier

Possible values: ENABLED, DISABLED Default value: DISABLED

trackAckOnlyPackets Track ack only packets as well. This setting is applicable only when packet rate limiting is being used.

Possible values: ENABLED, DISABLED Default value: DISABLED

trackTransactions Track transactions exceeding configured threshold. Transaction tracking can be enabled for following metric: ResponseTime. By default transaction tracking is disabled

Possible values: RESPTIME, NONE Default value: NONE

maxTransactionThreshold Maximum per transcation value of metric. Metric to be tracked is specified by tracktransactions attribute. Default value: 0 Minimum value: 0

minTransactionThreshold Minimum per transcation value of metric. Metric to be tracked is specified by tracktransactions attribute. Default value: 0 Minimum value: 0

acceptanceThreshold Non-Breaching transactions to Total transactions threshold expressed in percent. Maximum of 6 decimal places is supported. Default value: 0.000000

breachThreshold Breaching transactions threshold calculated over interval. Default value: 0 Minimum value: 0

Example

set stream identifier stream_id -selectorName top_clients -interval 1 -sampleCount 1 -sort NONE

unset stream identifier

Use this command to remove stream identifier settings.Refer to the set stream identifier command for meanings of the arguments.

Synopsis

unset stream identifier <name>

rm stream identifier

Removes a stream identifier. Note: You cannot remove a stream identifier if it is being used in a policy.

Synopsis

rm stream identifier <name>

Arguments

name The name of stream identifier.

Example

rm stream identifier stream_id

show stream identifier

Displays the parameters of the specified stream identifier or, if no stream identifier name is specified, the parameters of all configured stream identifiers.

Synopsis

show stream identifier

Arguments

name The name of stream identifier.

Output

selectorName Name of the selector to use with the stream identifier.

rule Rule.

ngname Nodegroup name to which this identifier belongs to.

recordlimit Maximum number of objects allowed per identifier.

interval Number of minutes of data to use when calculating session statistics (number of requests, bandwidth, and response times). The interval is a moving window that keeps the most recently collected data. Older data is discarded at regular intervals.

SampleCount Size of the sample from which to select a request for evaluation. The smaller the sample count, the more accurate is the statistical data. To evaluate all requests, set the sample count to 1. However, such a low setting can result in excessive consumption of memory and processing resources.

sort Sort stored records by the specified statistics column, in descending order. Performed during data collection, the sorting enables real-time data evaluation through Citrix ADC policies (for example, compression and caching policies) that use functions such as IS_TOP(n).

snmptrap Enable/disable SNMP trap for stream identifier

appflowLog Enable/disable Appflow logging for stream identifier

trackAckOnlyPackets Track ack only packets as well. This setting is applicable only when packet rate limiting is being used.

trackTransactions Track transactions exceeding configured threshold. Transaction tracking can be enabled for following metric: ResponseTime. By default transaction tracking is disabled

maxTransactionThreshold Maximum per transcation value of metric. Metric to be tracked is specified by tracktransactions attribute.

minTransactionThreshold Minimum per transcation value of metric. Metric to be tracked is specified by tracktransactions attribute.

acceptanceThreshold Non-Breaching transactions to Total transactions threshold expressed in percent. Maximum of 6 decimal places is supported.

breachThreshold Breaching transactions threshold calculated over interval.

log Location where objects collected on the identifier will be logged.

logInterval Time interval in minutes for logging the collected objects. Log interval should be greater than or equal to the inteval of the stream identifier.

logLimit Maximum number of objects to be logged in the log interval.

builtin Flag to determine if stream identifier is built-in or not

feature The feature to be checked while applying this config

stateflag used internally to identify ip addresses returned.

devno count

Example

show stream identifier stream_id

add stream identifier

Creates a stream identifier. A stream identifier specifies how data is collected and stored for an Action Analytics configuration.

Synopsis

add stream identifier <name> <selectorName> [-trackTransactions (RESPTIME | NONE)]

Arguments

name The name of stream identifier.

selectorName Name of the selector to use with the stream identifier.

interval Number of minutes of data to use when calculating session statistics (number of requests, bandwidth, and response times). The interval is a moving window that keeps the most recently collected data. Older data is discarded at regular intervals. Default value: 1 Minimum value: 1

SampleCount Size of the sample from which to select a request for evaluation. The smaller the sample count, the more accurate is the statistical data. To evaluate all requests, set the sample count to 1. However, such a low setting can result in excessive consumption of memory and processing resources. Default value: 1 Minimum value: 1 Maximum value: 65535

sort Sort stored records by the specified statistics column, in descending order. Performed during data collection, the sorting enables real-time data evaluation through Citrix ADC policies (for example, compression and caching policies) that use functions such as IS_TOP(n).

Possible values: REQUESTS, CONNECTIONS, RESPTIME, BANDWIDTH, RESPTIME_BREACHES, NONE Default value: REQUESTS

snmptrap Enable/disable SNMP trap for stream identifier

Possible values: ENABLED, DISABLED Default value: DISABLED

appflowLog Enable/disable Appflow logging for stream identifier

Possible values: ENABLED, DISABLED Default value: DISABLED

trackAckOnlyPackets Track ack only packets as well. This setting is applicable only when packet rate limiting is being used.

Possible values: ENABLED, DISABLED Default value: DISABLED

trackTransactions Track transactions exceeding configured threshold. Transaction tracking can be enabled for following metric: ResponseTime. By default transaction tracking is disabled

Possible values: RESPTIME, NONE Default value: NONE

maxTransactionThreshold Maximum per transcation value of metric. Metric to be tracked is specified by tracktransactions attribute. Default value: 0 Minimum value: 0

minTransactionThreshold Minimum per transcation value of metric. Metric to be tracked is specified by tracktransactions attribute. Default value: 0 Minimum value: 0

acceptanceThreshold Non-Breaching transactions to Total transactions threshold expressed in percent. Maximum of 6 decimal places is supported. Default value: 0.000000

breachThreshold Breaching transactions threshold calculated over interval. Default value: 0 Minimum value: 0

Example

add stream identifier stream_id top_url -interval 10 -sampleCount 1 -sort REQUESTS

stat stream identifier

Displays the statistics that the Citrix ADC has collected for the specified stream identifier.

Synopsis

stat stream identifier <name> [-sortBy <sortBy>]

Arguments

name Name of the stream identifier.

pattern Values on which grouping is performed are displayed in the output as row titles. If grouping is performed on two or more fields, their values are separated by a question mark in the row title.

For example, consider a selector that contains the expressions HTTP.REQ.URL and CLIENT.IP.SRC (in that order), on an appliance that has accumulated records of a number of

requests for two URLs, example.com/page1.html and example.com/page2.html, from two client IP addresses, 192.0.2.10 and 192.0.2.11.

With a pattern of ? ?, the appliance performs grouping on both fields and displays statistics for the following:

- Requests for example.com/abc.html from 192.0.2.10, with a row title of example.com/abc.html? 192.0.2.10.
- Requests for example.com/abc.html from 192.0.2.11, with a row title of example.com/abc.html? 192.0.2.11.
- Requests for example.com/def.html from 192.0.2.10, with a row title of example.com/def.html? 192.0.2.10.
- Requests for example.com/def.html from 192.0.2.11, with a row title of example.com/def.html? 192.0.2.11.

With a pattern of * ?, the appliance performs grouping on only the client IP address values and displays statistics for the following requests:

- All requests from 192.0.2.10, with the IP address as the row title.
- All requests from 192.0.2.11, with the IP address as the row title.

With a pattern of ? *, the appliance performs grouping on only the URL values and displays statistics for the following requests:

- All requests for example.com/abc.html, with the URL as the row title.
- All requests for example.com/def.html, with the URL as the row title.

With a pattern of * *, the appliance displays one set of collective statistics for all the requests received, with no row title.

With a pattern of example.com/abc.html ?, the appliance displays statistics for requests for example.com/abc.html from each unique client IP address.

With a pattern of * 192.0.2.11, the appliance displays statistics for all requests from 192.0.2.11.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

sortBy use this argument to sort by specific key

Possible values: Req, BandW, RspTime, Conn, breachcnt, pktCredits, pktsPerSecond, DroppedConns

sortOrder use this argument to specify sort order

Possible values: ascending, descending Default value: SORT_DESCENDING

Output

count devno stateflag

Counters

Stream Session Requests (Req) Total number of Stream Requests recieved.

Stream Session Bandwidth (BandW) Total Bandwidth consumed.

Stream Session Response Time (RspTime) Average response time of the stream session.

Stream Session Connections (Conn) Current connections on the stream session.

Stream Session Breaching Transactions (breachcnt) Total Breaching Transactions in configured interval.

Stream session packet credits (pktCredits) Calculated Packet credits on current connection.

Stream session packets per second (pktsPerSecond) Total packets recieved in configured interval.

Stream session connections dropped (DroppedConns) Total connections dropped.

stream-selector

The following operations can be performed on "stream-selector":

show| set| add| rm|

show stream selector

Displays the expressions configured for the specified selector or, if no selector name is specified, the expressions configured for all selectors.

Synopsis

show stream selector

Arguments

name Name for the selector. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. If the name includes one or more spaces, and you are using the Citrix ADC CLI, enclose the name in double or single quotation marks (for example, "my selector" or 'my selector').

Output

rule Set of up to five expressions. Maximum length: 7499 characters. Each expression must identify a specific request characteristic, such as the client's IP address (with CLIENT.IP.SRC) or requested server resource (with HTTP.REQ.URL). Note: If two or more selectors contain the same expressions in different order, a separate set of records is created for each selector.

builtin Flag to determine if stream selector is built-in or not

feature The feature to be checked while applying this config

stateflag devno count

Example

show ns limitSelector sel_subnet

set stream selector

Modifies the set of expressions in a stream selector. Note: You can change an expression if the selector is not yet being used in an identifier. If the selector is already in use, you can change only the order of the expressions, not the expressions themselves.

Synopsis

set stream selector <name> -rule <expression> ...

Arguments

name Name of the selector for which to modify parameters.

rule Set of up to five expressions. Maximum length: 7499 characters. Each expression must identify a specific request characteristic, such as the client's IP address (with CLIENT.IP.SRC) or requested server resource (with HTTP.REQ.URL). Note: If two or more selectors contain the same expressions in different order, a separate set of records is created for each selector.

Example

set stream sel_subnet HTTP.REQ.URL CLIENT.IP.SRC

add stream selector

Creates a selector for Action Analytics or traffic rate limiting.

Synopsis

add stream selector <name> <rule> ...

Arguments

name Name for the selector. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. If the name includes one or more spaces, and you are using the Citrix ADC CLI, enclose the name in double or single quotation marks (for example, "my selector" or 'my selector').

rule Set of up to five expressions. Maximum length: 7499 characters. Each expression must identify a specific request characteristic, such as the client's IP address (with CLIENT.IP.SRC) or requested server resource (with HTTP.REQ.URL). Note: If two or more selectors contain the same expressions in different order, a separate set of records is created for each selector.

Example

add stream selector sel_subnet HTTP.REQ.URL CLIENT.IP.SRC.SUBNET(24)

rm stream selector

Removes a selector. Note: Before you remove a selector, make sure that it is not being used by an identifier.

Synopsis

rm stream selector <name>

Arguments

name Name for the selector. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. If the name includes one or more spaces, and you are using the Citrix ADC CLI, enclose the name in double or single quotation marks (for example, "my selector" or 'my selector').

Example

rm stream selector sel_subnet

stream-session

The following operations can be performed on "stream-session":

clear stream session

Flushes all the records that have been accumulated for the specified stream identifier.

Synopsis

clear stream session <name>

Arguments

name Name of the stream identifier.

Example

clear stream session stream_id

subscriber

Subscriber

The entities on which you can perform NetScaler CLI operations:

- subscriber-gxInterface
- subscriber-param
- subscriber-profile
- subscriber-radiusInterface
- subscriber-sessions

subscriber-gxInterface

The following operations can be performed on "subscriber-gxInterface":

set| show| unset|

set subscriber gxInterface

Set the Gx Interface configuration on NS.

Synopsis

set subscriber gxInterface

Arguments

vServer Name of the load balancing, or content switching vserver to which the Gx connections are established. The service type of the virtual server must be DIAMETER/SSL_DIAMETER. Mutually exclusive with the service parameter. Therefore, you cannot set both service and the Virtual Server in the Gx Interface.

service Name of DIAMETER/SSL_DIAMETER service corresponding to PCRF to which the Gx connection is established. The service type of the service must be DIAMETER/SSL_DIAMETER. Mutually exclusive with vserver parameter. Therefore, you cannot set both Service and the Virtual Server in the Gx Interface.

pcrfRealm PCRF realm is of type DiameterIdentity and contains the realm of PCRF to which the message is to be routed. This is the realm used in Destination-Realm AVP by Citrix ADC Gx client (as a Diameter node).

holdOnSubscriberAbsence Set this setting to yes if Citrix ADC needs to Hold pakcets till subscriber session is fetched from PCRF. Else set to NO. By default set to yes. If this setting is set to NO, then till Citrix ADC fetches subscriber from PCRF, default subscriber profile will be applied to this subscriber if configured. If default subscriber profile is also not configured an undef would be raised to expressions which use Subscriber attributes.

Possible values: YES, NO Default value: YES

requestTimeout q!Time, in seconds, within which the Gx CCR request must complete. If the request does not complete within this time, the request is retransmitted for requestRetryAttempts time. If still reuqest is not complete then default subscriber profile will be applied to this subscriber if configured. If default subscriber profile is also not configured an undef would be raised to expressions which use Subscriber attributes. Zero disables the timeout. ! Default value: 10 Minimum value: 0 Maximum value: 86400

requestRetryAttempts If the request does not complete within requestTimeout time, the request is retransmitted for requestRetryAttempts time. Default value: 3 Minimum value: 0

revalidationTimeout q!Revalidation Timeout, in seconds, after which the Gx CCR-U request will be sent after any PCRF activity on a session. Any RAR or CCA message resets the timer. Zero value disables the idle timeout. ! Default value: 0 Minimum value: 0 Maximum value: 86400

healthCheck q!Set this setting to yes if Citrix ADC should send DWR packets to PCRF server. When the session is idle, healthcheck timer expires and DWR packets are initiated in order to check that PCRF server is active. By default set to No. !

Possible values: YES, NO Default value: NO

healthCheckTTL q!Healthcheck timeout, in seconds, after which the DWR will be sent in order to ensure the state of the PCRF server. Any CCR, CCA, RAR or RRA message resets the timer. ! Default value: 30 Minimum value: 6 Maximum value: 86400

cerRequestTimeout q!Healthcheck request timeout, in seconds, after which the Citrix ADC considers that no CCA packet received to the initiated CCR. After this time Citrix ADC should send again CCR to PCRF server. ! Default value: 0 Minimum value: 0 Maximum value: 86400

negativeTTL q!Negative TTL, in seconds, after which the Gx CCR-I request will be resent for sessions that have not been resolved by PCRF due to server being down or no response or failed response. Instead of polling the PCRF server constantly, negative-TTL makes Citrix ADC stick to un-resolved session. Meanwhile Citrix ADC installs a negative session to avoid going to PCRF. For Negative Sessions, Netcaler inherits the attributes from default subscriber profile if default subscriber is configured. A default subscriber could be configured as 'add subscriber profile *'. Or these attributes can be inherited from Radius as well if Radius is configued. Zero value disables the Negative Sessions. And Citrix ADC does not install Negative sessions even if subscriber session could not be fetched. ! Default value: 600 Minimum value: 0 Maximum value: 86400

negativeTTLLimitedSuccess Set this to YES if Citrix ADC should create negative session for Result-Code DIAMETER_LIMITED_SUCCESS (2002) received in CCA-I. If set to NO, regular session is created.

Possible values: YES, NO Default value: NO

purgeSDBonGxFailure Set this setting to YES if needed to purge Subscriber Database in case of Gx failure. By default set to NO.

Possible values: YES, NO Default value: NO

servicePathAVP The AVP code in which PCRF sends service path applicable for subscriber. Minimum value: 1

servicePathVendorid The vendorid of the AVP in which PCRF sends service path for subscriber. Minimum value: 0

show subscriber gxInterface

Displays the Gx interface parameters configured on the Citrix ADC.

Synopsis

show subscriber gxInterface

Arguments

Output

vServer Name of the load balancing, or content switching vserver to which the Gx connections are established. The service type of the virtual server must be DIAMETER/SSL_DIAMETER. Mutually

exclusive with the service parameter. Therefore, you cannot set both service and the Virtual Server in the Gx Interface.

service Name of DIAMETER/SSL_DIAMETER service corresponding to PCRF to which the Gx connection is established. The service type of the service must be DIAMETER/SSL_DIAMETER. Mutually exclusive with vserver parameter. Therefore, you cannot set both Service and the Virtual Server in the Gx Interface.

svrState The state of the gx service.

pcrfRealm PCRF realm is of type DiameterIdentity and contains the realm of PCRF to which the message is to be routed. This is the realm used in Destination-Realm AVP by Citrix ADC Gx client (as a Diameter node).

holdOnSubscriberAbsence Set this setting to yes if Citrix ADC needs to Hold pakcets till subscriber session is fetched from PCRF. Else set to NO. By default set to yes. If this setting is set to NO, then till Citrix ADC fetches subscriber from PCRF, default subscriber profile will be applied to this subscriber if configured. If default subscriber profile is also not configured an undef would be raised to expressions which use Subscriber attributes.

requestTimeout q!Time, in seconds, within which the Gx CCR request must complete. If the request does not complete within this time, the request is retransmitted for requestRetryAttempts time. If still reuqest is not complete then default subscriber profile will be applied to this subscriber if configured. If default subscriber profile is also not configured an undef would be raised to expressions which use Subscriber attributes. Zero disables the timeout. !

requestRetryAttempts If the request does not complete within requestTimeout time, the request is retransmitted for requestRetryAttempts time.

idleTTL q!Idle Time, in seconds, after which the Gx CCR-U request will be sent after any PCRF activity on a session. Any RAR or CCA message resets the timer. Zero value disables the idle timeout. !

revalidationTimeout q!Revalidation Timeout, in seconds, after which the Gx CCR-U request will be sent after any PCRF activity on a session. Any RAR or CCA message resets the timer. Zero value disables the idle timeout. !

healthCheck q!Set this setting to yes if Citrix ADC should send DWR packets to PCRF server. When the session is idle, healthcheck timer expires and DWR packets are initiated in order to check that PCRF server is active. By default set to No. !

healthCheckTTL q!Healthcheck timeout, in seconds, after which the DWR will be sent in order to ensure the state of the PCRF server. Any CCR, CCA, RAR or RRA message resets the timer. !

cerRequestTimeout q!Healthcheck request timeout, in seconds, after which the Citrix ADC considers that no CCA packet received to the initiated CCR. After this time Citrix ADC should send again CCR to PCRF server. !

negativeTTL q!Negative TTL, in seconds, after which the Gx CCR-I request will be resent for sessions that have not been resolved by PCRF due to server being down or no response or failed response. Instead of polling the PCRF server constantly, negative-TTL makes Citrix ADC stick to un-resolved session. Meanwhile Citrix ADC installs a negative session to avoid going to PCRF. For Negative Sessions, Netcaler inherits the attributes from default subscriber profile if default subscriber is configured. A default subscriber could be configured as 'add subscriber profile *'. Or these attributes can be inherited from Radius as well if Radius is configued. Zero value disables the Negative Sessions. And Citrix ADC does not install Negative sessions even if subscriber session could not be fetched. !

negativeTTLLimitedSuccess Set this to YES if Citrix ADC should create negative session for Result-Code DIAMETER_LIMITED_SUCCESS (2002) received in CCA-I. If set to NO, regular session is created.

purgeSDBonGxFailure Set this setting to YES if needed to purge Subscriber Database in case of Gx failure. By default set to NO.

identity DiameterIdentity to be used by NS. DiameterIdentity is used to identify a Diameter node uniquely. Before setting up diameter configuration, Citrix ADC (as a Diameter node) MUST be assigned a unique DiameterIdentity. example => set ns diameter -identity Citrix ADC.com Now whenever Citrix ADC system needs to use identity in diameter messages. It will use 'netscaler.com' as Origin-Host AVP as defined in RFC3588

realm Diameter Realm to be used by NS. example => set ns diameter -realm com Now whenever Citrix ADC system needs to use realm in diameter messages. It will use 'com' as Origin-Realm AVP as defined in RFC3588

status Citrix ADC PCRF connection Status. (Gx Protocol State)

servicePathAVP The AVP code in which PCRF sends service path applicable for subscriber.

servicePathVendorid The vendorid of the AVP in which PCRF sends service path for subscriber.

servicePathInfomode The type of info in which service path is passed from PCRF, SERVICE_FUNCTION: Denotes the service chain is passed as servicefunction names in-order in AVPS with code servicepathAVP SERVICE_PATH: Denotes the service path name is passed in AVPS with code servicepathAVP.q

gxReportingAvp1 The AVP code to report as 1st custom AVP.

gxReportingAvp1VendorId The vendorid of the AVP which will be reported as 1st custom AVP.

gxReportingAvp1Type The type of the AVP which will be reported as 1st custom AVP.

gxReportingAvp2 The AVP code to report as 2nd custom AVP.

gxReportingAvp2VendorId The vendorid of the AVP which will be reported as 2nd custom AVP.

gxReportingAvp2Type The type of the AVP which will be reported as 2nd custom AVP.

gxReportingAvp3 The AVP code to report as 3rd custom AVP.

gxReportingAvp3VendorId The vendorid of the AVP which will be reported as 3rd custom AVP.

gxReportingAvp3Type The type of the AVP which will be reported as 3rd custom AVP.

gxReportingAvp4 The AVP code to report as 4th custom AVP.

gxReportingAvp4VendorId The vendorid of the AVP which will be reported as 4th custom AVP.

gxReportingAvp4Type The type of the AVP which will be reported as 4th custom AVP.

gxReportingAvp5 The AVP code to report as 5th custom AVP.

gxReportingAvp5VendorId The vendorid of the AVP which will be reported as 5th custom AVP.

gxReportingAvp5Type The type of the AVP which will be reported as 5th custom AVP.

unset subscriber gxInterface

Use this command to remove subscriber gxInterface settings.Refer to the set subscriber gxInterface command for meanings of the arguments.

Synopsis

unset subscriber gxInterface

subscriber-param

The following operations can be performed on "subscriber-param":

set| unset| show|

set subscriber param

Modifies the subscriber params.

Synopsis

set subscriber param

Arguments

keytype Type of subscriber key type IP or IPANDVLAN. IPANDVLAN option can be used only when the interfaceType is set to gxOnly. Changing the lookup method should result to the subscriber session database being flushed.

Possible values: IP, IPANDVLAN Default value: IP

interfaceType Subscriber Interface refers to Citrix ADC interaction with control plane protocols, RADIUS and GX. Types of subscriber interface: NONE, RadiusOnly, RadiusAndGx, GxOnly. NONE: Only static subscribers can be configured. RadiusOnly: GX interface is absent. Subscriber information is obtained through RADIUS Accounting messages. RadiusAndGx: Subscriber ID obtained through RADIUS Accounting is used to query PCRF. Subscriber information is obtained from both RADIUS and PCRF. GxOnly: RADIUS interface is absent. Subscriber information is queried using Subscriber IP or IP+VLAN.

Possible values: None, RadiusOnly, RadiusAndGx, GxOnly Default value: None

idleTTL q!Idle Timeout, in seconds, after which Citrix ADC will take an idleAction on a subscriber session (refer to 'idleAction' arguement in 'set subscriber param' for more details on idleAction). Any data-plane or control plane activity updates the idleTimeout on subscriber session. idleAction could be to 'just delete the session' or 'delete and CCR-T' (if PCRF is configured) or 'do not delete but send a CCR-U'. Zero value disables the idle timeout. ! Default value: 0 Minimum value: 0 Maximum value: 172800

idleAction q!Once idleTTL exprires on a subscriber session, Citrix ADC will take an idle action on that session. idleAction could be chosen from one of these ==>

1. ccrTerminate: (default) send CCR-T to inform PCRF about session termination and delete the session.
2. delete: Just delete the subscriber session without informing PCRF.
3. ccrUpdate: Do not delete the session and instead send a CCR-U to PCRF requesting for an updated session. !

Possible values: ccrTerminate, delete, ccrUpdate Default value: ccrTerminate

ipv6PrefixLookupList The ipv6PrefixLookupList should consist of all the ipv6 prefix lengths assigned to the UE's' Minimum value: 1 Maximum value: 128

unset subscriber param

Use this command to remove subscriber param settings.Refer to the set subscriber param command for meanings of the arguments.

Synopsis

unset subscriber param

show subscriber param

displays global subscriber params.

Synopsis

show subscriber param

Arguments

Output

keytype Type of subscriber key type IP or IPANDVLAN. IPANDVLAN option can be used only when the interfaceType is set to gxOnly. Changing the lookup method should result to the subscriber session database being flushed.

interfaceType Subscriber Interface refers to Citrix ADC interaction with control plane protocols, RADIUS and GX. Types of subscriber interface: NONE, RadiusOnly, RadiusAndGx, GxOnly. NONE: Only static subscribers can be configured. RadiusOnly: GX interface is absent. Subscriber information is obtained through RADIUS Accounting messages. RadiusAndGx: Subscriber ID obtained through RADIUS Accounting is used to query PCRF. Subscriber information is obtained

from both RADIUS and PCRF. GxOnly: RADIUS interface is absent. Subscriber information is queried using Subscriber IP or IP+VLAN.

idleTTL q!Idle Timeout, in seconds, after which Citrix ADC will take an idleAction on a subscriber session (refer to 'idleAction' arguement in 'set subscriber param' for more details on idleAction). Any data-plane or control plane activity updates the idleTimeout on subscriber session. idleAction could be to 'just delete the session' or 'delete and CCR-T' (if PCRF is configured) or 'do not delete but send a CCR-U'. Zero value disables the idle timeout. !

idleAction q!Once idleTTL exprires on a subscriber session, Citrix ADC will take an idle action on that session. idleAction could be chosen from one of these ==>

1. ccrTerminate: (default) send CCR-T to inform PCRF about session termination and delete the session.
2. delete: Just delete the subscriber session without informing PCRF.
3. ccrUpdate: Do not delete the session and instead send a CCR-U to PCRF requesting for an updated session. !

ipv6PrefixLookupList The ipv6PrefixLookupList should consist of all the ipv6 prefix lengths assigned to the UE's'

builtin feature The feature to be checked while applying this config

subscriber-profile

The following operations can be performed on "subscriber-profile":

add| show| unset| rm| set|

add subscriber profile

Creates a static subscriber profile for mobile subscribers. When traffic passes through Citrix ADC, Citrix ADC can identify the subscribers for this traffic and Subscriber based policy expressions could be configured to enable subscriber aware traffic processing.

Synopsis

add subscriber profile <ip>@

Arguments

ip Subscriber ip address

vlan The vlan number on which the subscriber is located. Default value: 0 Minimum value: 0 Maximum value: 4096

subscriberRules Rules configured for this subscriber. This is similar to rules received from PCRF for dynamic subscriber sessions.

subscriptionIdType Subscription-Id type

Possible values: E164, IMSI, SIP_URI, NAI, PRIVATE

subscriptionIdvalue Subscription-Id value

servicePath Name of the servicepath to be taken for this subscriber.

Example

add subscriber profile 10.102.217.4 -subscriberRules rule1 rule2

show subscriber profile

show command of a static subscriber

Synopsis

show subscriber profile

Arguments

ip Subscriber ip address

vlan The vlan number on which the subscriber is located. Default value: 0 Minimum value: 0 Maximum value: 4096

Output

subscriptionIdType Subscription-Id type

subscriptionIdvalue Subscription-Id value

subscriberRules Rules configured for this subscriber. This is similar to rules received from PCRF for dynamic subscriber sessions.

stateflag Flags controlling the display.

flags Subscriber Session flags

TTL Subscriber Session TTL

avpdisplaybuffer Subscriber Attributes Display

servicePath Name of the servicepath to be taken for this subscriber.

devno count

Example

show subscriber profile 10.102.217.4

unset subscriber profile

Use this command to remove subscriber profile settings.Refer to the set subscriber profile command for meanings of the arguments.

Synopsis

unset subscriber profile <ip>@

rm subscriber profile

Deletes a static subscriber

Synopsis

rm subscriber profile <ip>@

Arguments

ip Subscriber ip address

vlan The vlan number on which the subscriber is located. Default value: 0 Minimum value: 0 Maximum value: 4096

Example

rm subscriber profile 10.102.217.4

set subscriber profile

Modifies a static subscriber

Synopsis

set subscriber profile <ip>@

Arguments

ip Subscriber ip address

vlan The vlan number on which the subscriber is located. Default value: 0 Minimum value: 0 Maximum value: 4096

subscriberRules Rules configured for this subscriber. This is similar to rules received from PCRF for dynamic subscriber sessions.

subscriptionIdType Subscription-Id type

Possible values: E164, IMSI, SIP_URI, NAI, PRIVATE

subscriptionIdvalue Subscription-Id value

servicePath Name of the servicepath to be taken for this subscriber.

Example

set subscriber profile 10.102.217.4 -subscriberRules rule1 rule2

subscriber-radiusInterface

The following operations can be performed on "subscriber-radiusInterface":

unset| show| set|

unset subscriber radiusInterface

Use this command to remove subscriber radiusInterface settings.Refer to the set subscriber radiusInterface command for meanings of the arguments.

Synopsis

unset subscriber radiusInterface -radiusInterimAsStart

show subscriber radiusInterface

Displays the RADIUS interface parameters configured on the Citrix ADC.

Synopsis

show subscriber radiusInterface

Arguments

Output

ListeningService Name of RADIUS LISTENING service that will process RADIUS accounting requests.

svrState The state of the radius service.

radiusInterimAsStart Treat radius interim message as start radius messages.

set subscriber radiusInterface

Set the RADIUS Interface configuration on NS.

Synopsis

set subscriber radiusInterface

Arguments

ListeningService Name of RADIUS LISTENING service that will process RADIUS accounting requests.

radiusInterimAsStart Treat radius interim message as start radius messages.

Possible values: ENABLED, DISABLED Default value: DISABLED

subscriber-sessions

The following operations can be performed on "subscriber-sessions":

show| clear|

show subscriber sessions

show command of a subscriber session

Synopsis

show subscriber sessions

Arguments

ip Subscriber IP Address.

vlan The vlan number on which the subscriber is located. Default value: 0 Minimum value: 0 Maximum value: 4096

Output

subscriptionIdType Subscription-Id type

subscriptionIdvalue Subscription-Id value

subscriberRules Rules stored in this session for this subscriber. When PCRF sends Charging-Rule-Name or Charging-Rule-Base-Name AVP for a subscriber, Citrix ADC stores these AVPs in the subscriber session. These Rules can be retreived using 'Subscriber.Rule_Active(<rule name>)' expression. For static subscriber profiles, these rules are configured using '-subscriberRules <list of rules>'.

stateflag Flags controlling the display.

flags Subscriber Session flags.

TTL Subscriber Session revalidation Timeout remaining. This TTL gets refreshed when a radius or CCA or RAR message is received for this subscriber session. Citrix ADC will send a CCR-U after revalidation timer expires. If subscriber sessions is a negative session, then Citrix ADC will send a CCR-I after TTL expires. Negative Sessions are sessions which have not been resolved by PCRF and instead of polling PCRF continously, Citrix ADC has installed a negative session. If default subscriber is configued, then Negative Sessions inherits default subscriber profile.

idleTTL Subscriber Session Activity Timeout remaining. Citrix ADC will take an idleAction after ttl expires. idleaction could be -->

1. ccrTerminate: (default) send CCR-T to inform PCRF about session termination and delete the session.
2. delete: Just delete the subscriber session without informing PCRF.
3. ccrUpdate: Do not delete the session and instead send a CCR-U to PCRF requesting for an updated session. But if this is a negative session and idleaction is ccrUpdate then Citrix ADC won't take any action. Also on negative sessions ccrTerminate translates to delete.

avpdisplaybuffer Subscriber Attributes Display.

servicePath Name of the servicepath to be taken for this subscriber.

devno count

Example

show subscriber session 10.102.217.4

clear subscriber sessions

Deletes a subscriber session. Without any arguement it clears the subscriber session database.

Synopsis

clear subscriber sessions

Arguments

ip Subscriber IP Address. Default value: 0

vlan The vlan number on which the subscriber is located. Default value: 0 Minimum value: 0 Maximum value: 4096

Example

clear subscriber session or \nclear subscriber session 3.3.3.3

system

system-admuserinfo

The following operations can be performed on "system-admuserinfo":

set system admuserinfo

Updates adm user name in the ssh session established between adm and adc.

Synopsis

set system admuserinfo -username <string>

Arguments

username Name of adm-user to log in syslogs.

system-autorestorefeature

The following operations can be performed on "system-autorestorefeature":

enable| disable|

enable system autorestorefeature

Enable the auto restore feature.

Synopsis

enable system autorestorefeature

disable system autorestorefeature

Disable the auto restore feature.

Synopsis

disable system autorestorefeature

system-backup

The following operations can be performed on "system-backup":

show| restore| rm| add| create|

show system backup

Retrieves the backed up files that were created in the appliance.

Synopsis

show system backup

Arguments

fileName Name of the backup file(*.tgz) to be restored. Maximum value: 67

Output

level Level of data to be backed up.

includekernel Use this option to add kernel in the backup file

comment Comment specified at the time of creation of the backup file(*.tgz).

size Size of the backup file(*.tgz) in KB.

useLocalTimezone This option will create backup file with local timezone timestamp

creationTime Creation time of the backup file(*.tgz).

version Build version of the backup file(*.tgz).

createdBy Name of user who created the backup file(*.tgz).

IPAddress Ip of Citrix ADC box where the backup file(*.tgz) was created.

devno count stateflag

restore system backup

Restores an appliance by using the backup file (*.tgz) that was created by using the "create system backup" command.

Synopsis

restore system backup <fileName>

Arguments

fileName Name of the backup file(*.tgz) to be restored. Maximum value: 67

skipbackup Use this option to skip taking backup during restore operation

rm system backup

Removes a backup file (*.tgz) that was created by using the "create system backup" command.

Synopsis

rm system backup <fileName>

Arguments

fileName Name of the backup file(*.tgz) to be restored. Maximum value: 67

add system backup

Adds a backup file (*.tgz) that was created in remote system by using the "create system backup" command.

Synopsis

add system backup <fileName>

Arguments

fileName Name of the backup file(*.tgz) to be restored. Maximum value: 67

create system backup

Creates a backup file (*.tgz) that is stored in the /var/ns_sys_backup/ directory. This file can be used to restore the appliance by using the "restore system backup" command.

Synopsis

create system backup

Arguments

fileName Name of the backup file(*.tgz) to be restored. Maximum value: 63

useLocalTimezone This option will create backup file with local timezone timestamp

level Level of data to be backed up.

Possible values: basic, full Default value: basic

includekernel Use this option to add kernel in the backup file

Possible values: NO, YES Default value: NO

comment Comment specified at the time of creation of the backup file(*.tgz).

system-bw

The following operations can be performed on "system-bw":

stat system bw

Displays BW statistics

Synopsis

stat system bw

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Number of HTTP Requests Sent (httpClttotpoolinactive) No of requests sent from BW client.

Number of HTTP responses received (httpCltotpooloutactive) No of responses Received.

Http responses (200 OK) (httpSvr200OKresp) Number of 200 Ok response sent from the BW appliance.

Http response error (404 NotFound) (httpSvr404ObjNotFound) Number of 404 Not Found responses sent

No of stray packets received without request (httpClterrstray) Number of stray packets received from server without HTTP request

RTT Value < 0.5 ms (httpCltTTFPBandLWM) Number of Responses Falling on LWM for TTFP.

RTT Value > 0.5 ms AND ' 1.5 ms (httpCltTTFPBand0) Number of Responses Falling on Band-0 for TTFP.

RTT Value > 1.5 ms AND ' 2.5 ms (httpCltTTFPBand1) Number of Responses Falling on Band-1 for TTFP.

RTT Value > 2.5 ms AND ' 3.5 ms (httpCltTTFPBand2) Number of Responses Falling on Band-2 for TTFP.

RTT Value > 3.5 ms AND ' 4.5 ms (httpCltTTFPBand3) Number of Responses Falling on Band-3 for TTFP.

RTT Value > 4.5 ms AND ' 5.5 ms (httpCltTTFPBand4) Number of Responses Falling on Band-4 for TTFP.

RTT Value > 5.5 ms AND ' 6.5 ms (httpCltTTFPBand5) Number of Responses Falling on Band-5 for TTFP.

RTT Value > 6.5 ms AND ' 7.5 ms (httpCltTTFPBand6) Number of Responses Falling on Band-6 for TTFP.

RTT Value > 7.5 ms AND ' 8.5 ms (httpCltTTFPBand7) Number of Responses Falling on Band-7 for TTFP.

RTT Value > 8.5 ms (httpCltTTFPBandHWM) Number of Responses Falling on HWM for TTFP.

TTFP Peak RTT (httpCltTTFPMax) Peak RTT observed for Time to First response packet.

RTT Value < 0.5 ms (httpCltTTLPBandLWM) Number of Responses Falling on LWM for TTLP.

RTT Value > 0.5 ms AND ' 1.5 ms (httpCltTTLPBand0) Number of Responses Falling on Band-0 for TTLP.

RTT Value > 1.5 ms AND ' 2.5 ms (httpCltTTLPBand1) Number of Responses Falling on Band-1 for TTLP.

RTT Value > 2.5 ms AND ' 3.5 ms (httpCltTTLPBand2) Number of Responses Falling on Band-2 for TTLP.

RTT Value > 3.5 ms AND ' 4.5 ms (httpCltTTLPBand3) Number of Responses Falling on Band-3 for TTLP.

RTT Value > 4.5 ms AND ' 5.5 ms (httpCltTTLPBand4) Number of Responses Falling on Band-4 for TTLP.

RTT Value > 5.5 ms AND ' 6.5 ms (httpCltTTLPBand5) Number of Responses Falling on Band-5 for TTLP.

RTT Value > 6.5 ms AND ' 7.5 ms (httpCltTTLPBand6) Number of Responses Falling on Band-6 for TTLP.

RTT Value > 7.5 ms AND ' 8.5 ms (httpCltTTLPBand7) Number of Responses Falling on Band-7 for TTLP.

RTT Value > 8.5 ms (httpCltTTLPBandHWM) Number of Responses Falling on HWM for TTLP.

TTLP peak RTT (httpCltTTLPMax) Peak RTT observed for Time to Last response packet.

Related Commands

- stat system memory

system-cmdPolicy

The following operations can be performed on "system-cmdPolicy":

add| rm| show| set|

add system cmdPolicy

Adds a command policy to the system. A command policy specifies the access rights of the system user. By default, the appliance already has the following policies defined:

- operator

- read-only
- network
- superuser

Synopsis

add system cmdPolicy <policyName> <action> <cmdSpec>

Arguments

policyName Name for a command policy. Must begin with a letter, number, or the underscore (_) character, and must contain only alphanumeric, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), and underscore characters. Cannot be changed after the policy is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

action Action to perform when a request matches the policy.

Possible values: ALLOW, DENY

cmdSpec Regular expression specifying the data that matches the policy.

rm system cmdPolicy

Removes a command policy from the appliance. Note: You cannot remove command policies that are bound to a system user.

Synopsis

rm system cmdPolicy <policyName>

Arguments

policyName Name of the command policy to remove.

show system cmdPolicy

Displays information about all configured system command policies, or about the specified policy.

Synopsis

show system cmdPolicy

Arguments

policyName Name of the system command policy about which to display information.

Output

action The policy action.

cmdSpec The matching rule that the policy will utilize.

builtin feature The feature to be checked while applying this config

devno count stateflag

set system cmdPolicy

Modifies the specified attributes of an existing command policy.

Synopsis

set system cmdPolicy <policyName> <action> <cmdSpec>

Arguments

policyName Name of the command policy to be modified.

action Action to perform when a request matches the policy.

Possible values: ALLOW, DENY

cmdSpec Regular expression specifying the data that matches the policy.

system-collectionparam

The following operations can be performed on "system-collectionparam":

unset| show| set|

unset system collectionparam

Use this command to remove system collectionparam settings.Refer to the set system collectionparam command for meanings of the arguments.

Synopsis

unset system collectionparam

show system collectionparam

Displays collection parameters for historical charting present in nscollect.ini file.

Synopsis

show system collectionparam

Arguments

Output

communityName SNMPv1 community name for authentication.

logLevel specify the log level. Possible values CRITICAL,WARNING,INFO,DEBUG1,DEBUG2

dataPath specify the data path to the database.

set system collectionparam

Modifies a collection parameters for historical charting in nscollect.ini file.

Synopsis

set system collectionparam

Arguments

logLevel specify the log level. Possible values CRITICAL,WARNING,INFO,DEBUG1,DEBUG2

dataPath specify the data path to the database.

System

The entities on which you can perform NetScaler CLI operations:

- system-admuserinfo
- system-autorestorefeature
- system-backup
- system-bw
- system-cmdPolicy
- system-collectionparam
- system-core

- system-countergroup
- system-counters
- system-cpu
- system-cpuparam
- system-dataSource
- system-entity
- system-entitydata
- system-entitytype
- system-eventhistory
- system-extramgmtcpu
- system-global
- system-globaldata
- system-group
- system-hwerror
- system-kek
- system-memory
- system-parameter
- system-restorepoint
- system-session
- system-sshkey
- system
- system-user

system-core

The following operations can be performed on "system-core":

show system core

Display entities in historical data.

Synopsis

show system core

Arguments

dataSource Specifies the source which contains all the stored counter values.

Output

response

system-countergroup

The following operations can be performed on "system-countergroup":

show system countergroup

Display available counter groups.

Synopsis

show system countergroup

Arguments

dataSource Specifies the source which contains all the stored counter values.

Output

response

system-counters

The following operations can be performed on "system-counters":

show system counters

Display entities in historical data.

Synopsis

show system counters

Arguments

countergroup Specify the (counter) group name which contains all the counters specific tot his particular group.

dataSource Specifies the source which contains all the stored counter values.

Output

response

system-cpu

The following operations can be performed on "system-cpu":

stat system cpu

Displays statistics of all CPUs available on the appliance, or statistics of the specified CPU.

Synopsis

stat system cpu

Arguments

id ID of the CPU for which to display statistics. Default value: 65535 Minimum value: 0 Maximum value: 65534

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

CPU Usage (Usage) CPU utilization percentage.

CPU Usage (Usage) CPU utilization percentage.

Related Commands

- stat system memory

system-cpuparam

The following operations can be performed on "system-cpuparam":

unset| show| set|

unset system cpuparam

Use this command to remove system cpuparam settings.Refer to the set system cpuparam command for meanings of the arguments.

Synopsis

unset system cpuparam -pemode

show system cpuparam

Displays PEmode state

Synopsis

show system cpuparam

Arguments

Output

pemode Set PEmode to DEFAULT/CPUBOUND. Distribute the PE weights equally if PEmode is set to CPUBOUND.

devno count stateflag

set system cpuparam

Set PEmode

Synopsis

set system cpuparam -pemode (DEFAULT | CPUBOUND)

Arguments

pemode Set PEmode to DEFAULT/CPUBOUND. Distribute the PE weights equally if PEmode is set to CPUBOUND.

Possible values: DEFAULT, CPUBOUND

system-dataSource

The following operations can be performed on "system-dataSource":

show system dataSource

Display entities in historical data.

Synopsis

show system dataSource

Arguments

dataSource Specifies the source which contains all the stored counter values.

Output

response

system-entity

The following operations can be performed on "system-entity":

show system entity

Display entities in historical data.

Synopsis

show system entity <type>

Arguments

type Specify the entity type.

dataSource Specifies the source which contains all the stored counter values.

core Specify core ID of the PE in nCore.

Output

response

Example

show system entity lbvserver

system-entitydata

The following operations can be performed on "system-entitydata":

rm| show|

rm system entitydata

Removes the specified entity from historical charting along with all the associated counters till the current time stamp.

Synopsis

rm system entitydata

Arguments

type Specify the entity type.

name Specify the entity name.

allDeleted Specify this if you would like to delete information about all deleted entities from the database.

allInactive Specify this if you would like to delete information about all inactive entities from the database.

dataSource Specifies the source which contains all the stored counter values.

core Specify core ID of the PE in nCore.

show system entitydata

Display the historical data for entity specific counters.

Synopsis

show system entitydata <type> <name> <counters> [-startTime <string> | (-last <integer>)]

Arguments

type Specify the entity type.

name Specify the entity name.

counters Specify the counters to be collected.

startTime Specify start time in mmddyyyyhhmm to start collecting values from that timestamp.

endTime Specify end time in mmddyyyyhhmm upto which values have to be collected.

last Last is literal way of saying a certain time period from the current moment. Example: -last 1 hour, -last 1 day, et cetera. Default value: 1

unit Specify the time period from current moment. Example 1 x where x = hours/ days/ years.

Possible values: HOURS, DAYS, MONTHS

dataSource Specifies the source which contains all the stored counter values.

core Specify core ID of the PE in nCore.

Output

response startUpdate lastupdate

Example

show system entitydata lbvserver v1 totalrequests -last 1 days

system-entitytype

The following operations can be performed on "system-entitytype":

show system entitytype

Display available entity types.

Synopsis

show system entitytype

Arguments

dataSource Specifies the source which contains all the stored counter values.

Output

response

system-eventhistory

The following operations can be performed on "system-eventhistory":

show system eventhistory

Display events in historical data.

Synopsis

show system eventhistory [-startTime <string> | (-last <integer>)] -dataSource <string>

Arguments

startTime Specify start time in mmddyyyyhhmm to start collecting values from that timestamp.

endTime Specify end time in mmddyyyyhhmm upto which values have to be collected.

last Last is literal way of saying a certain time period from the current moment. Example: -last 1 hour, -last 1 day, et cetera. Default value: 1

unit Specify the time period from current moment. Example 1 x where x = hours/ days/ years.

Possible values: HOURS, DAYS, MONTHS

dataSource Specifies the source which contains all the stored counter values.

Output

response

system-extramgmtcpu

The following operations can be performed on "system-extramgmtcpu":

show| enable| disable|

show system extramgmtcpu

Displays configured and effective state of Extra Management CPU. Configured and effective state will be different if command is fired but system is not rebooted

Synopsis

show system extramgmtcpu

Arguments

Output

ConfiguredState Get the configured state of extra manahement cpu

effectiveState Get the current running state of extra management cpu

enable system extramgmtcpu

Enables and dedicates extra CPU for Management from PE pool

Synopsis

enable system extramgmtcpu

disable system extramgmtcpu

Disables extra CPU for Management and returns back to the PE pool

Synopsis

disable system extramgmtcpu

system-global

The following operations can be performed on "system-global":

unbind| bind| show|

unbind system global

Unbinds a globally bound policy.

Synopsis

unbind system global <policyName>

Arguments

policyName Name of the globally bound policy to unbind.

bind system global

Binds policies globally.

Synopsis

bind system global [<policyName>]

Arguments

policyName Name of the policy to bind globally.

priority Integer specifying the priority of the policy. A lower number specifies a higher priority. Policies are evaluated in the order of their priority numbers. Note that priority range 64001 to 65535 is reserved for internal system usage of binding policies by default Minimum value: 0

nextFactor On success invoke label. Applicable for advanced authentication policy binding

gotoPriorityExpression Applicable only to advance authentication policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.

show system global

Displays information about all global policy bindings.

Synopsis

show system global

Arguments

Output

policyName The name of the command policy.

priority The priority of the command policy.

bindPolicyType Bound policy type

policySubType builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

stateflag globalBindType gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE. Applicable only for advanced authentication policies

nextFactor On success invoke label. Applicable for advanced authentication policy binding

devno count

system-globaldata

The following operations can be performed on "system-globaldata":

show system globaldata

Display historical data for global counters.

Synopsis

show system globaldata <counters> [-startTime <string> | (-last <integer>)]

Arguments

counters Specify the counters to be collected.

countergroup Specify the (counter) group name which contains all the counters specific to this particular group.

startTime Specify start time in mmddyyyyhhmm to start collecting values from that timestamp.

endTime Specify end time in mmddyyyyhhmm upto which values have to be collected.

last Last is literal way of saying a certain time period from the current moment. Example: -last 1 hour, -last 1 day, et cetera. Default value: 1

unit Specify the time period from current moment. Example 1 x where x = hours/ days/ years.

Possible values: HOURS, DAYS, MONTHS

dataSource Specifies the source which contains all the stored counter values.

core Specify core ID of the PE in nCore.

Output

response startUpdate lastupdate

Example

show system globaldata cpu_usage -last 1 hours

system-group

The following operations can be performed on "system-group":

unbind| add| unset| set| show| rm| bind|

unbind system group

Unbinds a system user from a group.

Synopsis

unbind system group <groupName> (-userName <string> | -policyName <string> | -partitionName <string>)

Arguments

groupName Name of the system group from which to unbind the user.

userName Name of the system user to unbind from the group.

policyName Command policy to unbind from the group.

partitionName Name of the Partition to bind to the system group.

add system group

Creates a system-user group, to which you can bind individual users by using the bind system group command.

Synopsis

add system group <groupName>

Arguments

groupName Name for the group. Must begin with a letter, number, hash(#) or the underscore (_) character, and must contain only alphanumeric, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), and underscore characters. Cannot be changed after the group is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my group" or 'my group').

promptString String to display at the command-line prompt. Can consist of letters, numbers, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), underscore (_), and the following variables:

- %u - Will be replaced by the user name.
- %h - Will be replaced by the hostname of the Citrix ADC.
- %t - Will be replaced by the current time in 12-hour format.
- %T - Will be replaced by the current time in 24-hour format.
- %d - Will be replaced by the current date.
- %s - Will be replaced by the state of the Citrix ADC.

Note: The 63-character limit for the length of the string does not apply to the characters that replace the variables.

timeout CLI session inactivity timeout, in seconds. If Restrictedtimeout argument of system parameter is enabled, Timeout can have values in the range seconds.If Restrictedtimeout argument of system parameter is disabled, Timeout can have values in the range seconds. Default value is 900 seconds.

allowedManagementInterface Allowed Management interfaces of the system users in the group. By default allowed from both API and CLI interfaces. If management interface for a group is set to API, then all users under this group will not allowed to access NS through CLI. GUI interface will come under API interface Default value: NS_INTERFACE_ALL

unset system group

Use this command to remove system group settings.Refer to the set system group command for meanings of the arguments.

Synopsis

unset system group <groupName>

set system group

Modifies the specified parameters of a system group.

Synopsis

set system group <groupName>

Arguments

groupName Name of system group to be modified.

promptString String to display at the command-line prompt. Can consist of letters, numbers, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), underscore (_), and the following variables:

- %u - Will be replaced by the user name.
- %h - Will be replaced by the hostname of the Citrix ADC.
- %t - Will be replaced by the current time in 12-hour format.
- %T - Will be replaced by the current time in 24-hour format.
- %d - Will be replaced by the current date.
- %s - Will be replaced by the state of the Citrix ADC.

Note: The 63-character limit for the length of the string does not apply to the characters that replace the variables.

timeout CLI session inactivity timeout, in seconds. If Restrictedtimeout argument of system parameter is enabled, Timeout can have values in the range seconds.If Restrictedtimeout argument of system parameter is disabled, Timeout can have values in the range seconds. Default value is 900 seconds.

allowedManagementInterface Allowed Management interfaces of the system users in the group. By default allowed from both API and CLI interfaces. If management interface for a group is set to API, then all users under this group will not allowed to access NS through CLI. GUI interface will come under API interface Default value: NS_INTERFACE_ALL

show system group

Displays information about all system groups configured on the appliance, or about the specified group.

Synopsis

show system group

Arguments

groupName Name of the system group about which to display information.

Output

userName The system user.

policyName The name of command policy.

priority The priority of the command policy.

promptString String to display at the command-line prompt. Can consist of letters, numbers, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), underscore (_), and the following variables:

- %u - Will be replaced by the user name.
- %h - Will be replaced by the hostname of the Citrix ADC.
- %t - Will be replaced by the current time in 12-hour format.
- %T - Will be replaced by the current time in 24-hour format.
- %d - Will be replaced by the current date.
- %s - Will be replaced by the state of the Citrix ADC.

Note: The 63-character limit for the length of the string does not apply to the characters that replace the variables.

timeout CLI session inactivity timeout, in seconds. If Restrictedtimeout argument of system parameter is enabled, Timeout can have values in the range seconds.If Restrictedtimeout argument of system parameter is disabled, Timeout can have values in the range seconds. Default value is 900 seconds.

partitionName Name of the Partition to bind to the system group.

allowedManagementInterface Allowed Management interfaces of the system users in the group. By default allowed from both API and CLI interfaces. If management interface for a group is set to API, then all users under this group will not allowed to access NS through CLI. GUI interface will come under API interface

devno count stateflag

rm system group

Removes a system group from the appliance.

Synopsis

rm system group <groupName>

Arguments

groupName Name of the system group to remove.

bind system group

Binds a system user to a system group.

Synopsis

bind system group <groupName> (-userName <string> | (-policyName <string> <priority>) | -partitionName <string>)

Arguments

groupName Name of the system group.

userName Name of a system user to bind to the group.

policyName Name of the command policy to be bind to the group.

priority Integer specifying the priority of the command policy. A lower number specifies a higher priority. Policies are evaluated in the order of their priority numbers. Minimum value: 0

partitionName Name of the Partition to bind to the system group.

system-hwerror

The following operations can be performed on "system-hwerror":

check system hwerror

Examines Citrix ADC for disk errors. The diskcheck parameter must be provided.

Synopsis

hwerrchk -diskCheck

Arguments

diskCheck Perform only disk error checking.

Output

response Response captured during hardware examination.

hwerrorCount Number of errors found. Check response field for more information on errors if this value is non zero.

Example

hwerrchk -diskCheck

system-kek

The following operations can be performed on "system-kek":

update system kek

updates the system KEK

Synopsis

update system kek -level (basic | extended)

Arguments

level Type of update KEK to be performed. *basic : The level basic will backup old keys and create new keys and respond back. *extended : The level extended will backup old keys and create new keys, update ns.conf, nscfg.db, all ns.conf for same release, in all partitions. While doing so will block all config changes and once done shall respond back.

Possible values: basic, extended

system-memory

The following operations can be performed on "system-memory":

stat system memory

Displays system-memory statistics.

Synopsis

stat system memory

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

InUse Memory (%) (cacmemMaxMemLimitPcnt) Integrated Cache memory insue percent.

InUse Memory (MB) (cacmemMaxMemLimit) Integrated Cache memory insue, in megabytes.

Maximum Allocation Failed (MB) (ShmemErrAllocFailed) Total shared memory allocation failed.

Shared Memory InUse (%) (shMemAllocpcnt) Shared memory insue percent.

Shared Memory InUse (MB) (shMemAllocMB) Shared memory insue, in megabytes.

Total Shared Memory (MB) (shMemtotMB) Total shared memory allowed to allocate, in megabytes.

Maximum Allocation Failed (MB) (MemTotAllocFailed) Total system memory allocation failed.

Free Memory (MB) (MemTotFree) Total Free PE Memory in the System.

InUse Memory (%) (MemUsage) Percentage of memory utilization on Citrix ADC.

InUse Memory (MB) (MemTotUseMB) Total Citrix ADC Memory in use, in megabytes.

Memory Allocated (%) (MemTotAlloc(%)) Currently allocated memory in percent.

Memory Allocated (MB) (MemTotAlloc) Currently allocated memory, in megabytes.

Memory Currently Available (MB) (MemTotMB) Total memory available (grabbed) for use by packet engine (PE), in megabytes.

Maximum Memory Available (MB) (MemTotAvail) Total system memory available for PE to grab from the system.

Maximum Memory (MB) (cacmemMaxSysLimitMB) Integrated Cache memory, in megabytes.

Maximum Memory Available (MB) (MemTotAvail) Total system memory available for PE to grab from the system.

Maximum Allocation Failed (MB) (MemTotAllocFailed) Total system memory allocation failed.

Total Shared Memory (MB) (shMemtotMB) Total shared memory allowed to allocate, in megabytes.

Shared Memory InUse (MB) (shMemAllocMB) Shared memory insue, in megabytes.

Maximum Allocation Failed (MB) (ShmemErrAllocFailed) Total shared memory allocation failed.

InUse Memory (MB) (cacmemMaxMemLimit) Integrated Cache memory insue, in megabytes.

Example

stat system memory

Related Commands

- stat system cpu

system-parameter

The following operations can be performed on "system-parameter":

unset| show| set|

unset system parameter

Resets the specified system parameters..Refer to the set system parameter command for meanings of the arguments.

Synopsis

unset system parameter

show system parameter

Displays information about the system parameters.

Synopsis

show system parameter

Arguments

Output

rbaOnResponse Enable or disable Role-Based Authentication (RBA) on responses.

promptString The global system prompt.

natPcbForceFlushLimit Flush the system if the number of Network Address Translation Protocol Control Blocks (NATPCBs) exceeds this value.

natPcbRstOnTimeout Send RST to client and server connections when the natpcbs timeout.This avoids the buildup of idle TCP connections on the both the sides.

timeout CLI session inactivity timeout, in seconds. If Restrictedtimeout argument is enabled, Timeout can have values in the range seconds. If Restrictedtimeout argument is disabled, Timeout can have values in the range seconds. Default value is 900 seconds.

maxClient Maximum number of client connection allowed by the system

localAuth When enabled, local users can access Citrix ADC even when external authentication is configured. When disabled, local users are not allowed to access the Citrix ADC, Local users can access the Citrix ADC only when the configured external authentication servers are unavailable. This parameter is not applicable to SSH Key-based authentication

minpasswordlen Minimum length of system user password. When strong password is enabled default minimum length is 8. User entered value can be greater than or equal to 8. Default mininum value is 1 when strong password is disabled. Maximum value is 127 in both cases.

strongpassword After enabling strong password (enableall / enablelocal - not included in exclude list), all the passwords / sensitive information must have - Atleast 1 Lower case character, Atleast 1 Upper case character, Atleast 1 numeric character, Atleast 1 special character (~, `, !, @, #, $, %, \^, &, *, -, _, =, +, {, }, , |, \, :, <, >, /, ., ,, " "). Exclude list in case of enablelocal is - NS_FIPS, NS_CRL, NS_RSAKEY, NS_PKCS12, NS_PKCS8, NS_LDAP, NS_TACACS,

NS_TACACSACTION, NS_RADIUS, NS_RADIUSACTION, NS_ENCRYPTION_PARAMS. So no Strong Password checks will be performed on these ObjectType commands for enablelocal case.

restrictedtimeout Enable/Disable the restricted timeout behaviour. When enabled, timeout cannot be configured beyond admin configured timeout and also it will have the range check. When disabled, timeout will have the old behaviour. By default the value is disabled

fipsUserMode Use this option to set the FIPS mode for key user-land processes. When enabled, these user-land processes will operate in FIPS mode. In this mode, these processes will use FIPS 140-2 certified crypto algorithms. With a FIPS license, it is enabled by default and cannot be disabled. Without a FIPS license, it is disabled by default, wherein these user-land processes will not operate in FIPS mode.

doppler Enable or disable Doppler

googleanalytics Enable or disable Google analytics

cliLoglevel Audit log level, which specifies the types of events to log for cli executed commands. Available values function as follows:

- EMERGENCY - Events that indicate an immediate crisis on the server.
- ALERT - Events that might require action.
- CRITICAL - Events that indicate an imminent server crisis.
- ERROR - Events that indicate some type of error.
- WARNING - Events that require action in the near future.
- NOTICE - Events that the administrator should know about.
- INFORMATIONAL - All but low-level events.
- DEBUG - All events, in extreme detail.

forcePasswordChange Enable or disable force password change for nsroot user

totalAuthTimeout Total time a request can take for authentication/authorization

basicAuth Enable or disable basic authentication for Nitro API.

allowDefaultPartition Enable/Disable the allowing partition users to access default partition

reauthOnAuthParamChange Enable or disable External user reauthentication when authentication parameter changes

removeSensitiveFiles Use this option to remove the sensitive files from the system like authorise keys, public keys etc. The commands which will remove sensitive files when this system paramter is enabled are rm cluster instance, rm cluster node, rm ha node, clear config full, join cluster and add cluster instance.

maxsessionperuser Maximum number of client connection allowed per user.The maxsessionperuser value ranges from 1 to 40

set system parameter

Modifies the specified system parameters.

Synopsis

set system parameter

Arguments

rbaOnResponse Enable or disable Role-Based Authentication (RBA) on responses.

Possible values: ENABLED, DISABLED Default value: ENABLED

promptString String to display at the command-line prompt. Can consist of letters, numbers, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), underscore (_), and the following variables:

- %u - Will be replaced by the user name.
- %h - Will be replaced by the hostname of the Citrix ADC.
- %t - Will be replaced by the current time in 12-hour format.
- %T - Will be replaced by the current time in 24-hour format.
- %d - Will be replaced by the current date.
- %s - Will be replaced by the state of the Citrix ADC.

Note: The 63-character limit for the length of the string does not apply to the characters that replace the variables.

natPcbForceFlushLimit Flush the system if the number of Network Address Translation Protocol Control Blocks (NATPCBs) exceeds this value. Default value: 2147483647 Minimum value: 1000

natPcbRstOnTimeout Send a reset signal to client and server connections when their NATPCBs time out. Avoids the buildup of idle TCP connections on both the sides.

Possible values: ENABLED, DISABLED Default value: DISABLED

timeout CLI session inactivity timeout, in seconds. If Restrictedtimeout argument is enabled, Timeout can have values in the range seconds. If Restrictedtimeout argument is disabled, Timeout can have values in the range seconds. Default value is 900 seconds.

localAuth When enabled, local users can access Citrix ADC even when external authentication is configured. When disabled, local users are not allowed to access the Citrix ADC, Local users can access the Citrix ADC only when the configured external authentication servers are unavailable. This parameter is not applicable to SSH Key-based authentication

Possible values: ENABLED, DISABLED Default value: ENABLED

minpasswordlen Minimum length of system user password. When strong password is enabled default minimum length is 8. User entered value can be greater than or equal to 8. Default mininum value is 1 when strong password is disabled. Maximum value is 127 in both cases. Minimum value: 1 Maximum value: 127

strongpassword After enabling strong password (enableall / enablelocal - not included in exclude list), all the passwords / sensitive information must have - Atleast 1 Lower case character, Atleast 1 Upper case character, Atleast 1 numeric character, Atleast 1 special character (~, `, !, @, #, $, %, \^, &, *, -, _, =, +, {, }, , |, \, :, <, >, /, ., ,, " "). Exclude list in case of enablelocal is - NS_FIPS, NS_CRL, NS_RSAKEY, NS_PKCS12, NS_PKCS8, NS_LDAP, NS_TACACS, NS_TACACSACTION, NS_RADIUS, NS_RADIUSACTION, NS_ENCRYPTION_PARAMS. So no Strong Password checks will be performed on these ObjectType commands for enablelocal case.

Possible values: enableall, enablelocal, disabled Default value: disabled

restrictedtimeout Enable/Disable the restricted timeout behaviour. When enabled, timeout cannot be configured beyond admin configured timeout and also it will have the range check. When disabled, timeout will have the old behaviour. By default the value is disabled

Possible values: ENABLED, DISABLED Default value: DISABLED

fipsUserMode Use this option to set the FIPS mode for key user-land processes. When enabled, these user-land processes will operate in FIPS mode. In this mode, these processes will use FIPS 140-2 certified crypto algorithms. With a FIPS license, it is enabled by default and cannot be disabled. Without a FIPS license, it is disabled by default, wherein these user-land processes will not operate in FIPS mode.

Possible values: ENABLED, DISABLED Default value: DISABLED

doppler Enable or disable Doppler

Possible values: ENABLED, DISABLED Default value: ENABLED

googleanalytics Enable or disable Google analytics

Possible values: ENABLED, DISABLED Default value: DISABLED

totalAuthTimeout Total time a request can take for authentication/authorization Default value: 20 Minimum value: 5 Maximum value: 120

cliLoglevel Audit log level, which specifies the types of events to log for cli executed commands. Available values function as follows:

- EMERGENCY - Events that indicate an immediate crisis on the server.
- ALERT - Events that might require action.
- CRITICAL - Events that indicate an imminent server crisis.
- ERROR - Events that indicate some type of error.
- WARNING - Events that require action in the near future.
- NOTICE - Events that the administrator should know about.
- INFORMATIONAL - All but low-level events.
- DEBUG - All events, in extreme detail.

Possible values: EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG Default value: INFORMATIONAL

forcePasswordChange Enable or disable force password change for nsroot user

Possible values: ENABLED, DISABLED Default value: DISABLED

basicAuth Enable or disable basic authentication for Nitro API.

Possible values: ENABLED, DISABLED Default value: ENABLED

reauthOnAuthParamChange Enable or disable External user reauthentication when authentication parameter changes

Possible values: ENABLED, DISABLED Default value: DISABLED

removeSensitiveFiles Use this option to remove the sensitive files from the system like authorise keys, public keys etc. The commands which will remove sensitive files when this system paramter

is enabled are rm cluster instance, rm cluster node, rm ha node, clear config full, join cluster and add cluster instance.

Possible values: ENABLED, DISABLED Default value: DISABLED

maxsessionperuser Maximum number of client connection allowed per user.The maxsessionperuser value ranges from 1 to 40 Minimum value: 1 Maximum value: 40

system-restorepoint

The following operations can be performed on "system-restorepoint":

show| create| rm|

show system restorepoint

Show the list of restore points. Right now maximum of 3 restorepoints are allowed

Synopsis

show system restorepoint

Arguments

fileName Name of the restore point. Maximum value: 63

Output

backupfilename backup file name of the restore points created internally

techsuprtname Tech support bundle name created during creation of restore points

creationTime Creation time of the restore points

version Build version of the restore points.

createdBy Name of user who created the restore points.

IPAddress Ip of Netscaler box where the restore point was created.

devno count stateflag

create system restorepoint

Create restore points which will be used to auto restore the system

Synopsis

create system restorepoint <fileName>

Arguments

fileName Name of the restore point. Maximum value: 63

rm system restorepoint

Removes a restore point that was created by using the "set restorepoint" command.

Synopsis

rm system restorepoint <fileName>

Arguments

fileName Name of the restore point. Maximum value: 63

system-session

The following operations can be performed on "system-session":

show| kill|

show system session

Displays information about all current system sessions, or about the specified session. The system might reclaim sessions with no active connections before expiry time.

Synopsis

show system session

Arguments

sid ID of the system session about which to display information. Minimum value: 1

Output

userName user name of the session

logintime logged-in time of this session

logintimelocal logged-in time (in local ADC timezone) of this session

lastactivitytime last activity time of this session

lastactivitytimelocal last activity time (in local ADC timezone) of this session

expirytime Time left in expire the session in seconds

numOfconnections number of connection using this token

currentconn True if the token is used for current session

clientType client type of the session

partitionName Name of the partition where the user is currently present.

clientIpAddress IP address of client connecting to ADC.

devno count stateflag

kill system session

Kills one system session, or all system sessions except the current session.

Synopsis

kill system session (<sid> | -all)

Arguments

sid ID of the system session to terminate.

CLI users: You can get the session ID by using the show system session command. Minimum value: 1

all Terminate all the system sessions except the current session.

system-sshkey

The following operations can be performed on "system-sshkey":

show| rm| import|

show system sshkey

Show the private key

Synopsis

show system sshkey

Arguments

sshkeytype The type of the ssh key whether public or private key

Possible values: PRIVATE, PUBLIC

Output

name URL \(protocol, host, path, and file name\) from where the location file will be imported. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

rm system sshkey

Remove the public or private key

Synopsis

rm system sshkey <name> -sshkeytype (PRIVATE | PUBLIC)

Arguments

name URL \(protocol, host, path, and file name\) from where the location file will be imported. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

sshkeytype The type of the ssh key whether public or private key

Possible values: PRIVATE, PUBLIC

import system sshkey

Import the ssh key.

Synopsis

import system sshkey <name> -src <URL> -sshkeytype (PRIVATE | PUBLIC)

Arguments

name URL \(protocol, host, path, and file name\) from where the location file will be imported. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

src URL \(protocol, host, path, and file name\) from where the location file will be imported. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access.

sshkeytype The type of the ssh key whether public or private key

Possible values: PRIVATE, PUBLIC

system-user

The following operations can be performed on "system-user":

show| unset| bind| add| rm| set| unbind|

show system user

Displays information about all system users configured on the appliance, or about the specified user.

Synopsis

show system user

Arguments

userName Name of a system user about whom to display information.

Output

groupName The system group.

policyName The name of command policy.

priority The priority of the policy.

password Password for the system user. Can include any ASCII character.

encrypted hashmethod externalAuth Whether to use external authentication servers for the system user authentication or not

promptString String to display at the command-line prompt. Can consist of letters, numbers, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), underscore (_), and the following variables:

- %u - Will be replaced by the user name.

- %h - Will be replaced by the hostname of the Citrix ADC.
- %t - Will be replaced by the current time in 12-hour format.
- %T - Will be replaced by the current time in 24-hour format.
- %d - Will be replaced by the current date.
- %s - Will be replaced by the state of the Citrix ADC.

Note: The 63-character limit for the length of the string does not apply to the characters that replace the variables.

promptInheritedFrom From where the prompt has been inherited.

timeout CLI session inactivity timeout, in seconds. If Restrictedtimeout argument of system parameter is enabled, Timeout can have values in the range seconds. If Restrictedtimeout argument of system parameter is disabled, Timeout can have values in the range seconds. Default value is 900 seconds.

timeoutKind From where the timeout has been inherited.

partitionName Name of the Partition to bind to the system user.

logging Users logging privilege

maxsession Maximum number of client connection allowed per user

allowedManagementInterface Allowed Management interfaces to the system user. By default user is allowed from both API and CLI interfaces. If management interface for a user is set to API, then user is not allowed to access NS through CLI. GUI interface will come under API interface

allowedManagementInterfaceKind Value of allowed interface which can be inherited from Global, Group or User.

devno count stateflag

unset system user

Resets the specified system user parameters.Refer to the set system user command for meanings of the arguments.

Synopsis

unset system user <userName>

bind system user

Binds a command policy or partition to a system user.

Synopsis

bind system user <userName> ((<policyName> <priority>) | -partitionName <string>)

Arguments

userName Name of the system-user entry to which to bind the command policy.

policyName Name of the command policy to bind to the system user.

priority Integer specifying the priority of the command policy. A lower number specifies a higher priority. Policies are evaluated in the order of their priority numbers. Minimum value: 0 Maximum value: 999999999

partitionName Name of the Partition to bind to the system user.

add system user

Adds a new user to the system. Note: You must provide the password after the user name.

Synopsis

add system user <userName>

Arguments

userName Name for a user. Must begin with a letter, number, or the underscore (_) character, and must contain only alphanumeric, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), and underscore characters. Cannot be changed after the user is added.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my user" or 'my user').

password Password for the system user. Can include any ASCII character.

externalAuth Whether to use external authentication servers for the system user authentication or not

Possible values: ENABLED, DISABLED Default value: ENABLED

promptString String to display at the command-line prompt. Can consist of letters, numbers, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), underscore (_), and the following variables:

- %u - Will be replaced by the user name.
- %h - Will be replaced by the hostname of the Citrix ADC.
- %t - Will be replaced by the current time in 12-hour format.
- %T - Will be replaced by the current time in 24-hour format.
- %d - Will be replaced by the current date.
- %s - Will be replaced by the state of the Citrix ADC.

Note: The 63-character limit for the length of the string does not apply to the characters that replace the variables.

timeout CLI session inactivity timeout, in seconds. If Restrictedtimeout argument of system parameter is enabled, Timeout can have values in the range seconds. If Restrictedtimeout argument of system parameter is disabled, Timeout can have values in the range seconds. Default value is 900 seconds.

logging Users logging privilege

Possible values: ENABLED, DISABLED Default value: DISABLED

maxsession Maximum number of client connection allowed per user Minimum value: 1 Maximum value: 40

allowedManagementInterface Allowed Management interfaces to the system user. By default user is allowed from both API and CLI interfaces. If management interface for a user is set to API, then user is not allowed to access NS through CLI. GUI interface will come under API interface Default value: NS_INTERFACE_ALL

rm system user

Removes a system user from the appliance.

Synopsis

rm system user <userName>

Arguments

userName Name of the system user to remove.

set system user

Modifies the specified parameters of a system-user entry.

Synopsis

set system user <userName> {-password }

Arguments

userName Name of the system-user entry to modify.

password Password for the system user. Can include any ASCII character.

externalAuth Whether to use external authentication servers for the system user authentication or not

Possible values: ENABLED, DISABLED Default value: ENABLED

promptString String to display at the command-line prompt. Can consist of letters, numbers, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), underscore (_), and the following variables:

- %u - Will be replaced by the user name.
- %h - Will be replaced by the hostname of the Citrix ADC.
- %t - Will be replaced by the current time in 12-hour format.
- %T - Will be replaced by the current time in 24-hour format.
- %d - Will be replaced by the current date.
- %s - Will be replaced by the state of the Citrix ADC.

Note: The 63-character limit for the length of the string does not apply to the characters that replace the variables.

timeout CLI session inactivity timeout, in seconds. If Restrictedtimeout argument of system parameter is enabled, Timeout can have values in the range seconds. If Restrictedtimeout argument of system parameter is disabled, Timeout can have values in the range seconds. Default value is 900 seconds.

logging Users logging privilege

Possible values: ENABLED, DISABLED Default value: DISABLED

maxsession Maximum number of client connection allowed per user Minimum value: 1 Maximum value: 40

allowedManagementInterface Allowed Management interfaces to the system user. By default user is allowed from both API and CLI interfaces. If management interface for a user is set to API, then user is not allowed to access NS through CLI. GUI interface will come under API interface Default value: NS_INTERFACE_ALL

unbind system user

Unbinds a command policy or partition from the system user.

Synopsis

unbind system user <userName> (<policyName> | -partitionName <string>)

Arguments

userName Name of the user entry from which to unbind the command policy.

policyName Name of the command policy to unbind.

partitionName Name of the Partition to unbind.

system

The following operations can be performed on "system":

stat system

This command displays system statistics

Synopsis

stat system

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

-12.0 V Supply Voltage (V12n) Power supply -12V output. Acceptable range is -13.20 through -10.80 volts. 9800 and 9960 platforms display standard value of -12.0V.

-5.0 V Supply Voltage (V50n) Power supply -5V output. Acceptable range is -5.50 through -4.50 volts. 9800 and 9960 platforms display standard value of -5.0V.

CPU usage (CPU) CPU utilization percentage.

Average CPU usage (CPU) Shows average CPU utilization percentage if more than 1 CPU is present.

CPU1 CPU 1 (currently the slave CPU) utilization, as percentage of capacity. Not applicable for a single-CPU system.

CPU0 CPU 0 (currently the master CPU) utilization, as percentage of capacity.

Voltage 7 (Volts) (volt7) Voltage of a device connected to health monitoring chip through pin 7.

Voltage 6 (Volts) (volt6) Voltage of a device connected to health monitoring chip through pin 6.

Voltage 5 (Volts) (volt5) Voltage of a device connected to health monitoring chip through pin 5.

Voltage 4 (Volts) (volt4) Voltage of a device connected to health monitoring chip through pin 4.

Voltage 3 (Volts) (volt3) Voltage of a device connected to health monitoring chip through pin 3.

Voltage 2 (Volts) (volt2) Voltage of a device connected to health monitoring chip through pin 2.

Voltage 1 (Volts) (volt1) Voltage of a device connected to health monitoring chip through pin 1.

Voltage 0 (Volts) (volt0) Voltage of a device connected to health monitoring chip through pin 0.

Voltage Sensor2(Volts) (VSEN2) Voltage Sensor 2 Input. Currently only 13k Platforms will have valid value for this counter and for older platforms this will be 0.

5V Standby Voltage(Volts) (V5SB) Power Supply 5V Standby Voltage. Currently only 13k Platforms will have valid value for this counter and for older platforms this will be 0.

Intel CPU Vtt Power(Volts) (VTT) Intel CPU Vtt power. Currently only 13k Platforms will have valid value for this counter and for older platforms this will be 0.

Battery Voltage (Volts) (VBAT) Onboard battery power supply output. 9800 and 9950 platforms display standard value of 5.0V.

+12.0 V Supply Voltage (V+12) Power supply +12V output. Acceptable range is 10.80 through 13.20 volts.

+5.0 V Supply Voltage (V50) Power supply +5V output. Acceptable range is 4.50 through 5.50 volts.

Standby 3.3 V Supply Voltage (V33Stby) Standby power supply +3.3V output. Acceptable range is 2.970 through 3.630 volts. 9800 and 9960 platforms display standard value of 3.3V. You can configure Standby 3.3V Supply Voltage by using the Set snmp alarm VOLTAGE-LOW command to set the lower limit and the Set snmp alarm VOLTAGE-HIGH command to set the upper limit.

Main 3.3 V Supply Voltage (V33Main) Main power supply +3.3V output. Acceptable range is 2.970 through 3.630 volts. This is a critical counter. You can configure Main 3.3V Supply Voltage, by using the Set snmp alarm VOLTAGE-LOW command to set the lower limit and the Set snmp alarm VOLTAGE-HIGH command to set the upper limit.

CPU 1 Core Voltage (Volts) (VCC1) CPU core 1 voltage. Acceptable range is 1.080 through 1.650 volts. If CPU 1 is not connected to the health monitoring chip, display shows voltage of CPU 0.

CPU 0 Core Voltage (Volts) (VCC0) CPU core 0 voltage. Acceptable range is 1.080 through 1.650 volts.

Number of CPUs (CPUs) The number of CPUs on the Citrix ADC.

InUse Memory (%) (MemUsage) Percentage of memory utilization on Citrix ADC.

Memory usage (MB) (MemUseMB) Main memory currently in use, in megabytes.

Mgmt Additional-CPU usage (%) (CPU) Additonal Management CPU utilization percentage.

Mgmt CPU0 usage (%) (CPU) Management CPU-0 utilization percentage.

Management CPU usage (%) (CPU) Average Management CPU utilization percentage.

Packet CPU usage (%) (CPU) Average CPU utilization percentage for all packet engines excluding management PE.

CPU usage (%) (CPU) CPU utilization percentage.

Average CPU usage (%) (CPU) Average CPU utilization percentage. Not applicable for a single-CPU system.

Up since(Local) (Since) Time (in local timezone format) when the Citrix ADC was last started.

Up since (Since) Time when the Citrix ADC was last started.

/flash Used (%) (disk0PerUsage) Used space in /flash partition of the disk, as a percentage. This is a critical counter. You can configure /flash Used (%) by using the Set snmp alarm DISK-USAGE-HIGH command.

/var Used (%) (disk1PerUsage) Used space in /var partition of the disk, as a percentage. This is a critical counter. You can configure /var Used (%) by using the Set snmp alarm DISK-USAGE-HIGH command.

CPU Fan 0 Speed (RPM) (CPUFan0) CPU Fan 0 speed. Acceptable range is 3000 through 6000 RPM. This is a critical counter. You can configure CPU Fan 0 Speed by using the Set snmp alarm FAN-SPEED-LOW command to set the lower limit.

CPU Fan 1 Speed (RPM) (CPUFan1) CPU Fan 1 speed. Acceptable range is 3000 through 6000 RPM. 7000 platform displays speed of CPU fan 0. This is a critical counter. You can configure CPU Fan 1 Speed by using the Set snmp alarm FAN-SPEED-LOW command to set the lower limit.

System Fan Speed (RPM) (systemFan) System fan speed. Acceptable range is 3000 through 6000 RPM. This is a critical counter. You can configure System Fan Speed by using the Set snmp alarm FAN-SPEED-LOW command to set the lower limit.

System Fan 1 Speed (RPM) (systemFan1) System fan 1 speed. For new platforms associated pin is connected to CPU supporting fans. For platforms in which it is not connected, it will point to System Fan.

System Fan 2 Speed (RPM) (systemFan2) System fan 2 speed. For new platforms associated pin is connected to CPU supporting fans. For platforms in which it is not connected, it will point to System Fan

CPU 0 Temperature (Celsius) (TCPU0) CPU 0 temperature. 9800 and 9960 platforms display internal chip temperature. This is a critical counter. You can configure CPU 0 Temperature by using the Set snmp alarm TEMPERATURE-HIGH command to set the upper limit.

CPU 1 Temperature (Celsius) (TCPU1) CPU 1 temperature. 9800 and 9960 platforms display internal chip temperature. 7000, 9010 and 10010 platforms display CPU 0 temperature. This is a critical counter. You can configure CPU 1 Temperature by using the Set snmp alarm TEMPERATURE-HIGH command to set the upper limit.

Internal Temperature (Celsius) (intTemp) Internal temperature of health monitoring chip. This is a critical counter. You can configure Internal Temperature by using the Set snmp alarm TEMPERATURE-HIGH command to set the upper limit.

Power supply 1 status (PS1FAIL) Power supply 1 failure status.

Power supply 2 status (PS2FAIL) Power supply 2 failure status.

Power supply 3 status (PS3FAIL) Power supply 3 failure status.

Power supply 4 status (PS4FAIL) Power supply 4 failure status.

/flash Size (MB) (disk0Size) Size of /flash partition of the hard disk.

/flash Used (MB) (disk0Used) Used space in /flash partition of the hard disk.

/flash Available (MB) (disk0Avail) Available space in /flash partition of the hard disk.

/var Size (MB) (disk1Size) Size of /var partition of the hard disk.

/var Used (MB) (disk1Used) Used space in /var partition of the hard disk.

/var Available (MB) (disk1Avail) Available space in /var partition of the hard disk.

Fan 0 Speed (RPM) (Fan0) Speed of Fan 0 if associated pin is connected to health monitoring chip.

Fan 1 Speed (RPM) (Fan1) Speed of Fan 1 if associated pin is connected to health monitoring chip.

Fan 2 Speed (RPM) (Fan2) Speed of Fan 2 if associated pin is connected to health monitoring chip.

Fan 3 Speed (RPM) (Fan3) Speed of Fan 3 if associated pin is connected to health monitoring chip.

Temperature 0 (Celsius) (temp0) Temperature of a device connected to health monitoring chip through pin 0.

Temperature 1 (Celsius) (temp1) Temperature of a device connected to health monitoring chip through pin 1.

Temperature 2 (Celsius) (temp2) Temperature of a device connected to health monitoring chip through pin 2.

Temperature 3 (Celsius) (temp3) Temperature of a device connected to health monitoring chip through pin 3.

Up time (UP) Seconds since the Citrix ADC started.

System memory (MB) (Memory) Total amount of system memory, in megabytes.

CPU usage (CPU) CPU utilization: percentage * 10.

Management CPU usage (CPU) Management CPU utilization: percentage * 10.

Management CPU0 usage (CPU) Management CPU-0 utilization: percentage * 10.

Additonal Management CPU usage (additionalCPU) Additonal Management CPU utilization: percentage * 10.

CPU 0 Core Voltage (Volts) (VCC0) CPU core 0 voltage. Acceptable range is 1.080 through 1.650 volts.

CPU 1 Core Voltage (Volts) (VCC1) CPU core 1 voltage. Acceptable range is 1.080 through 1.650 volts. If CPU 1 is not connected to the health monitoring chip, display shows voltage of CPU 0.

Main 3.3 V Supply Voltage (V33Main) Main power supply +3.3V output. Acceptable range is 2.970 through 3.630 volts. This is a critical counter. You can configure Main 3.3V Supply Voltage, by using the Set snmp alarm VOLTAGE-LOW command to set the lower limit and the Set snmp alarm VOLTAGE-HIGH command to set the upper limit.

Standby 3.3 V Supply Voltage (V33Stby) Standby power supply +3.3V output. Acceptable range is 2.970 through 3.630 volts. 9800 and 9960 platforms display standard value of 3.3V. You can configure Standby 3.3V Supply Voltage by using the Set snmp alarm VOLTAGE-LOW command to set the lower limit and the Set snmp alarm VOLTAGE-HIGH command to set the upper limit.

+5.0 V Supply Voltage (V50) Power supply +5V output. Acceptable range is 4.50 through 5.50 volts.

+12.0 V Supply Voltage (V+12) Power supply +12V output. Acceptable range is 10.80 through 13.20 volts.

Battery Voltage (Volts) (VBAT) Onboard battery power supply output. 9800 and 9950 platforms display standard value of 5.0V.

Intel CPU Vtt Power(Volts) (VTT) Intel CPU Vtt power. Currently only 13k Platforms will have valid value for this counter and for older platforms this will be 0.

5V Standby Voltage(Volts) (V5SB) Power Supply 5V Standby Voltage. Currently only 13k Platforms will have valid value for this counter and for older platforms this will be 0.

Voltage Sensor2(Volts) (VSEN2) Voltage Sensor 2 Input. Currently only 13k Platforms will have valid value for this counter and for older platforms this will be 0.

Voltage 0 (Volts) (volt0) Voltage of a device connected to health monitoring chip through pin 0.

Voltage 1 (Volts) (volt1) Voltage of a device connected to health monitoring chip through pin 1.

Voltage 2 (Volts) (volt2) Voltage of a device connected to health monitoring chip through pin 2.

Voltage 3 (Volts) (volt3) Voltage of a device connected to health monitoring chip through pin 3.

Voltage 4 (Volts) (volt4) Voltage of a device connected to health monitoring chip through pin 4.

Voltage 5 (Volts) (volt5) Voltage of a device connected to health monitoring chip through pin 5.

Voltage 6 (Volts) (volt6) Voltage of a device connected to health monitoring chip through pin 6.

Voltage 7 (Volts) (volt7) Voltage of a device connected to health monitoring chip through pin 7.

Master CPU usage (CPU0) CPU0 utilization: percentage * 10.

Slave CPU usage (CPU1) CPU1 utilization, percentage * 10.

-5.0 V Supply Voltage (V50n) Power supply -5V output. Acceptable range is -5.50 through -4.50 volts. 9800 and 9960 platforms display standard value of -5.0V.

-12.0 V Supply Voltage (V12n) Power supply -12V output. Acceptable range is -13.20 through -10.80 volts. 9800 and 9960 platforms display standard value of -12.0V.

Related Commands

- stat system memory

tm

Tm

The entities on which you can perform NetScaler CLI operations:

- tm-formSSOAction
- tm-global
- tm-samlSSOProfile
- tm-sessionAction
- tm-sessionParameter
- tm-sessionPolicy
- tm-trafficAction
- tm-trafficPolicy

tm-formSSOAction

The following operations can be performed on "tm-formSSOAction":

set| rm| unset| add| show|

set tm formSSOAction

Modifies the specified attributes of a form-based single sign-on traffic profile (action.)

Synopsis

set tm formSSOAction <name>

Arguments

name Name of the form-based single sign-on profile (action) to modify.

actionURL URL to which the completed form is submitted.

userField Name of the form field in which the user types in the user ID.

passwdField Name of the form field in which the user types in the password.

ssoSuccessRule Expression, that checks to see if single sign-on is successful.

responsesize Number of bytes, in the response, to parse for extracting the forms. Default value: 8096 Minimum value: 0

nameValuePair Name-value pair attributes to send to the server in addition to sending the username and password. Value names are separated by an ampersand (&) (for example, name1=value1&name2=value2).

nvtype Type of processing of the name-value pair. If you specify STATIC, the values configured by the administrator are used. For DYNAMIC, the response is parsed, and the form is extracted and then submitted.

Possible values: STATIC, DYNAMIC Default value: DYNAMIC

submitMethod HTTP method used by the single sign-on form to send the logon credentials to the logon server. Applies only to STATIC name-value type.

Possible values: GET, POST Default value: GET

rm tm formSSOAction

Deletes an existing form-based single sign-on traffic profile (action.)

Synopsis

rm tm formSSOAction <name>

Arguments

name Name of the form-based single sign-on profile to delete.

unset tm formSSOAction

Use this command to remove tm formSSOAction settings.Refer to the set tm formSSOAction command for meanings of the arguments.

Synopsis

unset tm formSSOAction <name>

add tm formSSOAction

Creates a form-based single sign-on traffic profile (action.) Form-based single sign-on allows users to access web applications that require an HTML form-based logon without having to type their password again for each new application.

Synopsis

add tm formSSOAction <name> -actionURL <URL> -userField <string> -passwdField <string> -ssoSuccessRule <expression>

Arguments

name Name for the new form-based single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

actionURL URL to which the completed form is submitted.

userField Name of the form field in which the user types in the user ID.

passwdField Name of the form field in which the user types in the password.

ssoSuccessRule Expression, that checks to see if single sign-on is successful.

nameValuePair Name-value pair attributes to send to the server in addition to sending the username and password. Value names are separated by an ampersand (&) (for example, name1=value1&name2=value2).

responsesize Number of bytes, in the response, to parse for extracting the forms. Default value: 8096 Minimum value: 0

nvtype Type of processing of the name-value pair. If you specify STATIC, the values configured by the administrator are used. For DYNAMIC, the response is parsed, and the form is extracted and then submitted.

Possible values: STATIC, DYNAMIC Default value: DYNAMIC

submitMethod HTTP method used by the single sign-on form to send the logon credentials to the logon server. Applies only to STATIC name-value type.

Possible values: GET, POST Default value: GET

show tm formSSOAction

Displays information about all configured form-based single sign-on actions, or displays detailed information about the specified action.

Synopsis

show tm formSSOAction

Arguments

name Name of the SSO action for which to display detailed information.

Output

actionURL URL to which the completed form is submitted.

userField Username field.

passwdField Password field.

responsesize Number of bytes, in the response, to parse for extracting the forms.

nameValuePair Form attributes and their values to be submitted.

nvtype Bypass Form extraction

ssoSuccessRule Rule to be evaluated to check whether sso succeeded or not.

submitMethod Form Submit method.

devno count stateflag

tm-global

The following operations can be performed on "tm-global":

show| unbind| bind|

show tm global

Displays information about TM global bindings.

Synopsis

show tm global

Arguments

Output

policyName The name of the policy.

priority The priority of the policy.

type Bindpoint to which the policy is bound

policySubType stateflag builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

bindPolicyType Bound policy type

globalBindType gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

devno count

unbind tm global

Unbinds a globally bound traffic session policy.

Synopsis

unbind tm global -policyName <string>

Arguments

policyName Name of the policy to unbind.

bind tm global

Binds traffic, sessions, nslog, and syslog policies to traffic management (TM) Global.

Synopsis

bind tm global [-policyName <string>]

Arguments

policyName Name of the policy that you are binding.

priority Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Minimum value: 0

gotoPriorityExpression Applicable only to advance tmsession policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

tm-samlSSOProfile

The following operations can be performed on "tm-samlSSOProfile":

set| show| add| rm| unset|

set tm samlSSOProfile

Modifies the specified attributes of a saml single sign-on traffic profile.

Synopsis

set tm samlSSOProfile <name> [-Attribute1 <string> -Attribute1Expr <string>] [-Attribute2 <string> -Attribute2Expr <string>] [-Attribute3 <string> -Attribute3Expr <string>] [-Attribute4 <string> -Attribute4Expr <string>] [-Attribute5 <string> -Attribute5Expr <string>] [-Attribute6 <string> -Attribute6Expr <string>] [-Attribute7 <string> -Attribute7Expr <string>] [-Attribute8 <string> -Attribute8Expr <string>] [-Attribute9 <string> -Attribute9Expr <string>] [-Attribute10 <string> -Attribute10Expr <string>] [-Attribute11 <string> -Attribute11Expr <string>] [-Attribute12 <string> -Attribute12Expr <string>] [-Attribute13 <string> -Attribute13Expr <string>] [-Attribute14 <string> -Attribute14Expr <string>] [-Attribute15 <string> -Attribute15Expr <string>] [-Attribute16 <string> -Attribute16Expr <string>]

Arguments

name Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

samlSigningCertName Name of the SSL certificate that is used to Sign Assertion.

assertionConsumerServiceURL URL to which the assertion is to be sent.

samlIssuerName The name to be used in requests sent fromCitrix ADC to IdP to uniquely identify Citrix ADC.

relaystateRule Expression to extract relaystate to be sent along with assertion. Evaluation of this expression should return TEXT content. This is typically a targ et url to which user is redirected after the recipient validates SAML token

signatureAlg Algorithm to be used to sign/verify SAML transactions

Possible values: RSA-SHA1, RSA-SHA256 Default value: RSA-SHA256

digestMethod Algorithm to be used to compute/verify digest for SAML transactions

Possible values: SHA1, SHA256 Default value: SHA256

audience Audience for which assertion sent by IdP is applicable. This is typically entity name or url that represents ServiceProvider

NameIDFormat Format of Name Identifier sent in Assertion.

Possible values: Unspecified, emailAddress, X509SubjectName, WindowsDomainQualifiedName, kerberos, entity, persistent, transient Default value: transient

NameIDExpr Expression that will be evaluated to obtain NameIdentifier to be sent in assertion

Attribute1 Name of attribute1 that needs to be sent in SAML Assertion

Attribute1Expr Expression that will be evaluated to obtain attribute1's value to be sent in Assertion

Attribute1FriendlyName User-Friendly Name of attribute1 that needs to be sent in SAML Assertion

Attribute1Format Format of Attribute1 to be sent in Assertion.

Possible values: URI, Basic

Attribute2 Name of attribute2 that needs to be sent in SAML Assertion

Attribute2Expr Expression that will be evaluated to obtain attribute2's value to be sent in Assertion

Attribute2FriendlyName User-Friendly Name of attribute2 that needs to be sent in SAML Assertion

Attribute2Format Format of Attribute2 to be sent in Assertion.

Possible values: URI, Basic

Attribute3 Name of attribute3 that needs to be sent in SAML Assertion

Attribute3Expr Expression that will be evaluated to obtain attribute3's value to be sent in Assertion

Attribute3FriendlyName User-Friendly Name of attribute3 that needs to be sent in SAML Assertion

Attribute3Format Format of Attribute3 to be sent in Assertion.

Possible values: URI, Basic

Attribute4 Name of attribute4 that needs to be sent in SAML Assertion

Attribute4Expr Expression that will be evaluated to obtain attribute4's value to be sent in Assertion

Attribute4FriendlyName User-Friendly Name of attribute4 that needs to be sent in SAML Assertion

Attribute4Format Format of Attribute4 to be sent in Assertion.

Possible values: URI, Basic

Attribute5 Name of attribute5 that needs to be sent in SAML Assertion

Attribute5Expr Expression that will be evaluated to obtain attribute5's value to be sent in Assertion

Attribute5FriendlyName User-Friendly Name of attribute5 that needs to be sent in SAML Assertion

Attribute5Format Format of Attribute5 to be sent in Assertion.

Possible values: URI, Basic

Attribute6 Name of attribute6 that needs to be sent in SAML Assertion

Attribute6Expr Expression that will be evaluated to obtain attribute6's value to be sent in Assertion

Attribute6FriendlyName User-Friendly Name of attribute6 that needs to be sent in SAML Assertion

Attribute6Format Format of Attribute6 to be sent in Assertion.

Possible values: URI, Basic

Attribute7 Name of attribute7 that needs to be sent in SAML Assertion

Attribute7Expr Expression that will be evaluated to obtain attribute7's value to be sent in Assertion

Attribute7FriendlyName User-Friendly Name of attribute7 that needs to be sent in SAML Assertion

Attribute7Format Format of Attribute7 to be sent in Assertion.

Possible values: URI, Basic

Attribute8 Name of attribute8 that needs to be sent in SAML Assertion

Attribute8Expr Expression that will be evaluated to obtain attribute8's value to be sent in Assertion

Attribute8FriendlyName User-Friendly Name of attribute8 that needs to be sent in SAML Assertion

Attribute8Format Format of Attribute8 to be sent in Assertion.

Possible values: URI, Basic

Attribute9 Name of attribute9 that needs to be sent in SAML Assertion

Attribute9Expr Expression that will be evaluated to obtain attribute9's value to be sent in Assertion

Attribute9FriendlyName User-Friendly Name of attribute9 that needs to be sent in SAML Assertion

Attribute9Format Format of Attribute9 to be sent in Assertion.

Possible values: URI, Basic

Attribute10 Name of attribute10 that needs to be sent in SAML Assertion

Attribute10Expr Expression that will be evaluated to obtain attribute10's value to be sent in Assertion

Attribute10FriendlyName User-Friendly Name of attribute10 that needs to be sent in SAML Assertion

Attribute10Format Format of Attribute10 to be sent in Assertion.

Possible values: URI, Basic

Attribute11 Name of attribute11 that needs to be sent in SAML Assertion

Attribute11Expr Expression that will be evaluated to obtain attribute11's value to be sent in Assertion

Attribute11FriendlyName User-Friendly Name of attribute11 that needs to be sent in SAML Assertion

Attribute11Format Format of Attribute11 to be sent in Assertion.

Possible values: URI, Basic

Attribute12 Name of attribute12 that needs to be sent in SAML Assertion

Attribute12Expr Expression that will be evaluated to obtain attribute12's value to be sent in Assertion

Attribute12FriendlyName User-Friendly Name of attribute12 that needs to be sent in SAML Assertion

Attribute12Format Format of Attribute12 to be sent in Assertion.

Possible values: URI, Basic

Attribute13 Name of attribute13 that needs to be sent in SAML Assertion

Attribute13Expr Expression that will be evaluated to obtain attribute13's value to be sent in Assertion

Attribute13FriendlyName User-Friendly Name of attribute13 that needs to be sent in SAML Assertion

Attribute13Format Format of Attribute13 to be sent in Assertion.

Possible values: URI, Basic

Attribute14 Name of attribute14 that needs to be sent in SAML Assertion

Attribute14Expr Expression that will be evaluated to obtain attribute14's value to be sent in Assertion

Attribute14FriendlyName User-Friendly Name of attribute14 that needs to be sent in SAML Assertion

Attribute14Format Format of Attribute14 to be sent in Assertion.

Possible values: URI, Basic

Attribute15 Name of attribute15 that needs to be sent in SAML Assertion

Attribute15Expr Expression that will be evaluated to obtain attribute15's value to be sent in Assertion

Attribute15FriendlyName User-Friendly Name of attribute15 that needs to be sent in SAML Assertion

Attribute15Format Format of Attribute15 to be sent in Assertion.

Possible values: URI, Basic

Attribute16 Name of attribute16 that needs to be sent in SAML Assertion

Attribute16Expr Expression that will be evaluated to obtain attribute16's value to be sent in Assertion

Attribute16FriendlyName User-Friendly Name of attribute16 that needs to be sent in SAML Assertion

Attribute16Format Format of Attribute16 to be sent in Assertion.

Possible values: URI, Basic

encryptAssertion Option to encrypt assertion when Citrix ADC sends one.

Possible values: ON, OFF Default value: OFF

samlSPCertName Name of the SSL certificate of peer/receving party using which Assertion is encrypted.

encryptionAlgorithm Algorithm to be used to encrypt SAML assertion

Possible values: DES3, AES128, AES192, AES256 Default value: AES256

skewTime This option specifies the number of minutes on either side of current time that the assertion would be valid. For example, if skewTime is 10, then assertion would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all. Default value: 5

signAssertion Option to sign portions of assertion when Citrix ADC IDP sends one. Based on the user selection, either Assertion or Response or Both or none can be signed

Possible values: NONE, ASSERTION, RESPONSE, BOTH Default value: ASSERTION

show tm samlSSOProfile

Displays information about all configured saml single sign-on profiles, or displays detailed information about the specified action.

Synopsis

show tm samlSSOProfile

Arguments

name Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period

(.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

Output

samlSigningCertName Name of the SSL certificate that is used to Sign Assertion.

assertionConsumerServiceURL URL to which the assertion is to be sent.

sendPassword Option to send password in assertion.

samlIssuerName The name to be used in requests sent fromCitrix ADC to IdP to uniquely identify Citrix ADC.

relaystateRule Expression to extract relaystate to be sent along with assertion. Evaluation of this expression should return TEXT content. This is typically a targ et url to which user is redirected after the recipient validates SAML token

signatureAlg Algorithm to be used to sign/verify SAML transactions

digestMethod Algorithm to be used to compute/verify digest for SAML transactions

audience Audience for which assertion sent by IdP is applicable. This is typically entity name or url that represents ServiceProvider

NameIDFormat Format of Name Identifier sent in Assertion.

NameIDExpr Expression that will be evaluated to obtain NameIdentifier to be sent in assertion

Attribute1 Name of attribute1 that needs to be sent in SAML Assertion

Attribute2 Name of attribute2 that needs to be sent in SAML Assertion

Attribute3 Name of attribute3 that needs to be sent in SAML Assertion

Attribute4 Name of attribute4 that needs to be sent in SAML Assertion

Attribute5 Name of attribute5 that needs to be sent in SAML Assertion

Attribute6 Name of attribute6 that needs to be sent in SAML Assertion

Attribute7 Name of attribute7 that needs to be sent in SAML Assertion

Attribute8 Name of attribute8 that needs to be sent in SAML Assertion

Attribute9 Name of attribute9 that needs to be sent in SAML Assertion

Attribute10 Name of attribute10 that needs to be sent in SAML Assertion

Attribute11 Name of attribute11 that needs to be sent in SAML Assertion

Attribute12 Name of attribute12 that needs to be sent in SAML Assertion

Attribute13 Name of attribute13 that needs to be sent in SAML Assertion

Attribute14 Name of attribute14 that needs to be sent in SAML Assertion

Attribute15 Name of attribute15 that needs to be sent in SAML Assertion

Attribute16 Name of attribute16 that needs to be sent in SAML Assertion

Attribute1FriendlyName User-Friendly Name of attribute1 that needs to be sent in SAML Assertion

Attribute2FriendlyName User-Friendly Name of attribute2 that needs to be sent in SAML Assertion

Attribute3FriendlyName User-Friendly Name of attribute3 that needs to be sent in SAML Assertion

Attribute4FriendlyName User-Friendly Name of attribute4 that needs to be sent in SAML Assertion

Attribute5FriendlyName User-Friendly Name of attribute5 that needs to be sent in SAML Assertion

Attribute6FriendlyName User-Friendly Name of attribute6 that needs to be sent in SAML Assertion

Attribute7FriendlyName User-Friendly Name of attribute7 that needs to be sent in SAML Assertion

Attribute8FriendlyName User-Friendly Name of attribute8 that needs to be sent in SAML Assertion

Attribute9FriendlyName User-Friendly Name of attribute9 that needs to be sent in SAML Assertion

Attribute10FriendlyName User-Friendly Name of attribute10 that needs to be sent in SAML Assertion

Attribute11FriendlyName User-Friendly Name of attribute11 that needs to be sent in SAML Assertion

Attribute12FriendlyName User-Friendly Name of attribute12 that needs to be sent in SAML Assertion

Attribute13FriendlyName User-Friendly Name of attribute13 that needs to be sent in SAML Assertion

Attribute14FriendlyName User-Friendly Name of attribute14 that needs to be sent in SAML Assertion

Attribute15FriendlyName User-Friendly Name of attribute15 that needs to be sent in SAML Assertion

Attribute16FriendlyName User-Friendly Name of attribute16 that needs to be sent in SAML Assertion

Attribute1Format Format of Attribute1 to be sent in Assertion.

Attribute2Format Format of Attribute2 to be sent in Assertion.

Attribute3Format Format of Attribute3 to be sent in Assertion.

Attribute4Format Format of Attribute4 to be sent in Assertion.

Attribute5Format Format of Attribute5 to be sent in Assertion.

Attribute6Format Format of Attribute6 to be sent in Assertion.

Attribute7Format Format of Attribute7 to be sent in Assertion.

Attribute8Format Format of Attribute8 to be sent in Assertion.

Attribute9Format Format of Attribute9 to be sent in Assertion.

Attribute10Format Format of Attribute10 to be sent in Assertion.

Attribute11Format Format of Attribute11 to be sent in Assertion.

Attribute12Format Format of Attribute12 to be sent in Assertion.

Attribute13Format Format of Attribute13 to be sent in Assertion.

Attribute14Format Format of Attribute14 to be sent in Assertion.

Attribute15Format Format of Attribute15 to be sent in Assertion.

Attribute16Format Format of Attribute16 to be sent in Assertion.

Attribute1Expr Expression that will be evaluated to obtain attribute1's value to be sent in Assertion

Attribute2Expr Expression that will be evaluated to obtain attribute2's value to be sent in Assertion

Attribute3Expr Expression that will be evaluated to obtain attribute3's value to be sent in Assertion

Attribute4Expr Expression that will be evaluated to obtain attribute4's value to be sent in Assertion

Attribute5Expr Expression that will be evaluated to obtain attribute5's value to be sent in Assertion

Attribute6Expr Expression that will be evaluated to obtain attribute6's value to be sent in Assertion

Attribute7Expr Expression that will be evaluated to obtain attribute7's value to be sent in Assertion

Attribute8Expr Expression that will be evaluated to obtain attribute8's value to be sent in Assertion

Attribute9Expr Expression that will be evaluated to obtain attribute9's value to be sent in Assertion

Attribute10Expr Expression that will be evaluated to obtain attribute10's value to be sent in Assertion

Attribute11Expr Expression that will be evaluated to obtain attribute11's value to be sent in Assertion

Attribute12Expr Expression that will be evaluated to obtain attribute12's value to be sent in Assertion

Attribute13Expr Expression that will be evaluated to obtain attribute13's value to be sent in Assertion

Attribute14Expr Expression that will be evaluated to obtain attribute14's value to be sent in Assertion

Attribute15Expr Expression that will be evaluated to obtain attribute15's value to be sent in Assertion

Attribute16Expr Expression that will be evaluated to obtain attribute16's value to be sent in Assertion

encryptAssertion Option to encrypt assertion when Citrix ADC sends one.

samlSPCertName Name of the SSL certificate of peer/receving party using which Assertion is encrypted.

encryptionAlgorithm Algorithm to be used to encrypt SAML assertion

skewTime This option specifies the number of minutes on either side of current time that the assertion would be valid. For example, if skewTime is 10, then assertion would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all.

signAssertion Option to sign portions of assertion when Citrix ADC IDP sends one. Based on the user selection, either Assertion or Response or Both or none can be signed

devno count stateflag

add tm samlSSOProfile

Creates a SAML single sign-on profile. This profile is employed in triggering saml assertion to a target service based on traffic profile.

Synopsis

add tm samlSSOProfile <name> -assertionConsumerServiceURL <URL> [-Attribute1 <string> -Attribute1Expr <string>] [-Attribute2 <string> -Attribute2Expr <string>] [-Attribute3 <string> -Attribute3Expr <string>] [-Attribute4 <string> -Attribute4Expr <string>] [-Attribute5 <string> -Attribute5Expr <string>] [-Attribute6 <string> -Attribute6Expr <string>] [-Attribute7 <string> -Attribute7Expr <string>] [-Attribute8 <string> -Attribute8Expr <string>] [-Attribute9 <string> -Attribute9Expr <string>] [-Attribute10 <string> -Attribute10Expr <string>] [-Attribute11 <string> -Attribute11Expr <string>] [-Attribute12 <string> -Attribute12Expr <string>] [-Attribute13 <string> -Attribute13Expr <string>] [-Attribute14 <string> -Attribute14Expr <string>] [-Attribute15 <string> -Attribute15Expr <string>] [-Attribute16 <string> -Attribute16Expr <string>]

Arguments

name Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

samlSigningCertName Name of the SSL certificate that is used to Sign Assertion.

assertionConsumerServiceURL URL to which the assertion is to be sent.

relaystateRule Expression to extract relaystate to be sent along with assertion. Evaluation of this expression should return TEXT content. This is typically a targ et url to which user is redirected after the recipient validates SAML token

samlIssuerName The name to be used in requests sent fromCitrix ADC to IdP to uniquely identify Citrix ADC.

signatureAlg Algorithm to be used to sign/verify SAML transactions

Possible values: RSA-SHA1, RSA-SHA256 Default value: RSA-SHA256

digestMethod Algorithm to be used to compute/verify digest for SAML transactions

Possible values: SHA1, SHA256 Default value: SHA256

audience Audience for which assertion sent by IdP is applicable. This is typically entity name or url that represents ServiceProvider

NameIDFormat Format of Name Identifier sent in Assertion.

Possible values: Unspecified, emailAddress, X509SubjectName, WindowsDomainQualifiedName, kerberos, entity, persistent, transient Default value: transient

NameIDExpr Expression that will be evaluated to obtain NameIdentifier to be sent in assertion

Attribute1 Name of attribute1 that needs to be sent in SAML Assertion

Attribute1Expr Expression that will be evaluated to obtain attribute1's value to be sent in Assertion

Attribute1FriendlyName User-Friendly Name of attribute1 that needs to be sent in SAML Assertion

Attribute1Format Format of Attribute1 to be sent in Assertion.

Possible values: URI, Basic

Attribute2 Name of attribute2 that needs to be sent in SAML Assertion

Attribute2Expr Expression that will be evaluated to obtain attribute2's value to be sent in Assertion

Attribute2FriendlyName User-Friendly Name of attribute2 that needs to be sent in SAML Assertion

Attribute2Format Format of Attribute2 to be sent in Assertion.

Possible values: URI, Basic

Attribute3 Name of attribute3 that needs to be sent in SAML Assertion

Attribute3Expr Expression that will be evaluated to obtain attribute3's value to be sent in Assertion

Attribute3FriendlyName User-Friendly Name of attribute3 that needs to be sent in SAML Assertion

Attribute3Format Format of Attribute3 to be sent in Assertion.

Possible values: URI, Basic

Attribute4 Name of attribute4 that needs to be sent in SAML Assertion

Attribute4Expr Expression that will be evaluated to obtain attribute4's value to be sent in Assertion

Attribute4FriendlyName User-Friendly Name of attribute4 that needs to be sent in SAML Assertion

Attribute4Format Format of Attribute4 to be sent in Assertion.

Possible values: URI, Basic

Attribute5 Name of attribute5 that needs to be sent in SAML Assertion

Attribute5Expr Expression that will be evaluated to obtain attribute5's value to be sent in Assertion

Attribute5FriendlyName User-Friendly Name of attribute5 that needs to be sent in SAML Assertion

Attribute5Format Format of Attribute5 to be sent in Assertion.

Possible values: URI, Basic

Attribute6 Name of attribute6 that needs to be sent in SAML Assertion

Attribute6Expr Expression that will be evaluated to obtain attribute6's value to be sent in Assertion

Attribute6FriendlyName User-Friendly Name of attribute6 that needs to be sent in SAML Assertion

Attribute6Format Format of Attribute6 to be sent in Assertion.

Possible values: URI, Basic

Attribute7 Name of attribute7 that needs to be sent in SAML Assertion

Attribute7Expr Expression that will be evaluated to obtain attribute7's value to be sent in Assertion

Attribute7FriendlyName User-Friendly Name of attribute7 that needs to be sent in SAML Assertion

Attribute7Format Format of Attribute7 to be sent in Assertion.

Possible values: URI, Basic

Attribute8 Name of attribute8 that needs to be sent in SAML Assertion

Attribute8Expr Expression that will be evaluated to obtain attribute8's value to be sent in Assertion

Attribute8FriendlyName User-Friendly Name of attribute8 that needs to be sent in SAML Assertion

Attribute8Format Format of Attribute8 to be sent in Assertion.

Possible values: URI, Basic

Attribute9 Name of attribute9 that needs to be sent in SAML Assertion

Attribute9Expr Expression that will be evaluated to obtain attribute9's value to be sent in Assertion

Attribute9FriendlyName User-Friendly Name of attribute9 that needs to be sent in SAML Assertion

Attribute9Format Format of Attribute9 to be sent in Assertion.

Possible values: URI, Basic

Attribute10 Name of attribute10 that needs to be sent in SAML Assertion

Attribute10Expr Expression that will be evaluated to obtain attribute10's value to be sent in Assertion

Attribute10FriendlyName User-Friendly Name of attribute10 that needs to be sent in SAML Assertion

Attribute10Format Format of Attribute10 to be sent in Assertion.

Possible values: URI, Basic

Attribute11 Name of attribute11 that needs to be sent in SAML Assertion

Attribute11Expr Expression that will be evaluated to obtain attribute11's value to be sent in Assertion

Attribute11FriendlyName User-Friendly Name of attribute11 that needs to be sent in SAML Assertion

Attribute11Format Format of Attribute11 to be sent in Assertion.

Possible values: URI, Basic

Attribute12 Name of attribute12 that needs to be sent in SAML Assertion

Attribute12Expr Expression that will be evaluated to obtain attribute12's value to be sent in Assertion

Attribute12FriendlyName User-Friendly Name of attribute12 that needs to be sent in SAML Assertion

Attribute12Format Format of Attribute12 to be sent in Assertion.

Possible values: URI, Basic

Attribute13 Name of attribute13 that needs to be sent in SAML Assertion

Attribute13Expr Expression that will be evaluated to obtain attribute13's value to be sent in Assertion

Attribute13FriendlyName User-Friendly Name of attribute13 that needs to be sent in SAML Assertion

Attribute13Format Format of Attribute13 to be sent in Assertion.

Possible values: URI, Basic

Attribute14 Name of attribute14 that needs to be sent in SAML Assertion

Attribute14Expr Expression that will be evaluated to obtain attribute14's value to be sent in Assertion

Attribute14FriendlyName User-Friendly Name of attribute14 that needs to be sent in SAML Assertion

Attribute14Format Format of Attribute14 to be sent in Assertion.

Possible values: URI, Basic

Attribute15 Name of attribute15 that needs to be sent in SAML Assertion

Attribute15Expr Expression that will be evaluated to obtain attribute15's value to be sent in Assertion

Attribute15FriendlyName User-Friendly Name of attribute15 that needs to be sent in SAML Assertion

Attribute15Format Format of Attribute15 to be sent in Assertion.

Possible values: URI, Basic

Attribute16 Name of attribute16 that needs to be sent in SAML Assertion

Attribute16Expr Expression that will be evaluated to obtain attribute16's value to be sent in Assertion

Attribute16FriendlyName User-Friendly Name of attribute16 that needs to be sent in SAML Assertion

Attribute16Format Format of Attribute16 to be sent in Assertion.

Possible values: URI, Basic

encryptAssertion Option to encrypt assertion when Citrix ADC sends one.

Possible values: ON, OFF Default value: OFF

samlSPCertName Name of the SSL certificate of peer/receving party using which Assertion is encrypted.

encryptionAlgorithm Algorithm to be used to encrypt SAML assertion

Possible values: DES3, AES128, AES192, AES256 Default value: AES256

skewTime This option specifies the number of minutes on either side of current time that the assertion would be valid. For example, if skewTime is 10, then assertion would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all. Default value: 5

signAssertion Option to sign portions of assertion when Citrix ADC IDP sends one. Based on the user selection, either Assertion or Response or Both or none can be signed

Possible values: NONE, ASSERTION, RESPONSE, BOTH Default value: ASSERTION

rm tm samlSSOProfile

Deletes an existing saml single sign-on traffic profile.

Synopsis

rm tm samlSSOProfile <name>

Arguments

name Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

unset tm samlSSOProfile

Use this command to remove tm samlSSOProfile settings.Refer to the set tm samlSSOProfile command for meanings of the arguments.

Synopsis

unset tm samlSSOProfile <name>

tm-sessionAction

The following operations can be performed on "tm-sessionAction":

add| show| unset| rm| set|

add tm sessionAction

Creates a session action (profile) that allows you to override global settings for any of the session parameters.

Synopsis

add tm sessionAction <name>

Arguments

name Name for the session action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after a session action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

sessTimeout Session timeout, in minutes. If there is no traffic during the timeout period, the user is disconnected and must reauthenticate to access intranet resources. Minimum value: 1

defaultAuthorizationAction Allow or deny access to content for which there is no specific authorization policy.

Possible values: ALLOW, DENY

SSO Use single sign-on (SSO) to log users on to all web applications automatically after they authenticate, or pass users to the web application logon page to authenticate to each application individually. Note that this configuration does not honor the following authentication types for security reason. BASIC, DIGEST, and NTLM (without Negotiate NTLM2 Key or Negotiate Sign Flag). Use TM TrafficAction to configure SSO for these authentication types.

Possible values: ON, OFF Default value: OFF

ssoCredential Use the primary or secondary authentication credentials for single sign-on (SSO).

Possible values: PRIMARY, SECONDARY

ssoDomain Domain to use for single sign-on (SSO).

httpOnlyCookie Allow only an HTTP session cookie, in which case the cookie cannot be accessed by scripts.

Possible values: YES, NO Default value: YES

kcdAccount Kerberos constrained delegation account name

persistentCookie Enable or disable persistent SSO cookies for the traffic management (TM) session. A persistent cookie remains on the user device and is sent with each HTTP request. The cookie becomes stale if the session ends. This setting is overwritten if a traffic action sets persistent cookie to OFF. Note: If persistent cookie is enabled, make sure you set the persistent cookie validity.

Possible values: ON, OFF

persistentCookieValidity Integer specifying the number of minutes for which the persistent cookie remains valid. Can be set only if the persistent cookie setting is enabled. Minimum value: 1

homePage Web address of the home page that a user is displayed when authentication vserver is bookmarked and used to login.

show tm sessionAction

Displays information about all configured traffic management (TM) session actions, or detailed information about the specified TM session action.

Synopsis

show tm sessionAction

Arguments

name Name of the existing traffic management (TM) session action for which to display detailed information.

Output

sessTimeout The session timeout, in minutes, set by the action.

defaultAuthorizationAction The Authorization Action, e.g. allow or deny

stateflag SSO Whether or not Single Sign-On is used for this session.

ssoCredential Use the primary or secondary authentication credentials for single sign-on (SSO).

ssoDomain Domain to use for single sign-on (SSO).

kcdAccount Kerberos constrained delegation account name

httpOnlyCookie Allow only an HTTP session cookie, in which case the cookie cannot be accessed by scripts.

persistentCookie Enable or disable persistent SSO cookies for the traffic management (TM) session. A persistent cookie remains on the user device and is sent with each HTTP request. The cookie becomes stale if the session ends. This setting is overwritten if a traffic action sets persistent cookie to OFF. Note: If persistent cookie is enabled, make sure you set the persistent cookie validity.

persistentCookieValidity Integer specifying the number of minutes for which the persistent cookie remains valid. Can be set only if the persistent cookie setting is enabled.

homePage Web address of the home page that a user is displayed when authentication vserver is bookmarked and used to login.

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

devno count

unset tm sessionAction

Use this command to remove tm sessionAction settings.Refer to the set tm sessionAction command for meanings of the arguments.

Synopsis

unset tm sessionAction <name>

rm tm sessionAction

Deletes an existing session action.

Synopsis

rm tm sessionAction <name>

Arguments

name Name of the session action to delete.

set tm sessionAction

Modifies the specified parameters of an existing session action.

Synopsis

set tm sessionAction <name>

Arguments

name Name of the session action to modify.

sessTimeout Session timeout, in minutes. If there is no traffic during the timeout period, the user is disconnected and must reauthenticate to access intranet resources. Minimum value: 1

defaultAuthorizationAction Allow or deny access to content for which there is no specific authorization policy.

Possible values: ALLOW, DENY

SSO Use single sign-on (SSO) to log users on to all web applications automatically after they authenticate, or pass users to the web application logon page to authenticate to each application individually. Note that this configuration does not honor the following authentication types for security reason. BASIC, DIGEST, and NTLM (without Negotiate NTLM2 Key or Negotiate Sign Flag). Use TM TrafficAction to configure SSO for these authentication types.

Possible values: ON, OFF Default value: OFF

ssoCredential Use the primary or secondary authentication credentials for single sign-on (SSO).

Possible values: PRIMARY, SECONDARY

ssoDomain Domain to use for single sign-on (SSO).

kcdAccount Kerberos constrained delegation account name

httpOnlyCookie Allow only an HTTP session cookie, in which case the cookie cannot be accessed by scripts.

Possible values: YES, NO Default value: YES

persistentCookie Enable or disable persistent SSO cookies for the traffic management (TM) session. A persistent cookie remains on the user device and is sent with each HTTP request. The cookie becomes stale if the session ends. This setting is overwritten if a traffic action sets persistent cookie to OFF. Note: If persistent cookie is enabled, make sure you set the persistent cookie validity.

Possible values: ON, OFF

persistentCookieValidity Integer specifying the number of minutes for which the persistent cookie remains valid. Can be set only if the persistent cookie setting is enabled. Minimum value: 1

homePage Web address of the home page that a user is displayed when authentication vserver is bookmarked and used to login.

tm-sessionParameter

The following operations can be performed on "tm-sessionParameter":

set| show| unset|

set tm sessionParameter

Sets global parameters for the traffic management (TM) session. Parameters defined when adding a traffic session action override these parameters.

Synopsis

set tm sessionParameter

Arguments

sessTimeout Session timeout, in minutes. If there is no traffic during the timeout period, the user is disconnected and must reauthenticate to access the intranet resources. Default value: 30 Minimum value: 1

defaultAuthorizationAction Allow or deny access to content for which there is no specific authorization policy.

Possible values: ALLOW, DENY Default value: DENY

SSO Log users on to all web applications automatically after they authenticate, or pass users to the web application logon page to authenticate for each application. Note that this configuration does not honor the following authentication types for security reason. BASIC, DIGEST, and NTLM (without Negotiate NTLM2 Key or Negotiate Sign Flag). Use TM TrafficAction to configure SSO for these authentication types.

Possible values: ON, OFF Default value: OFF

ssoCredential Use primary or secondary authentication credentials for single sign-on.

Possible values: PRIMARY, SECONDARY Default value: PRIMARY

ssoDomain Domain to use for single sign-on.

kcdAccount Kerberos constrained delegation account name

httpOnlyCookie Allow only an HTTP session cookie, in which case the cookie cannot be accessed by scripts.

Possible values: YES, NO Default value: YES

persistentCookie Use persistent SSO cookies for the traffic session. A persistent cookie remains on the user device and is sent with each HTTP request. The cookie becomes stale if the session ends.

Possible values: ON, OFF Default value: OFF

persistentCookieValidity Integer specifying the number of minutes for which the persistent cookie remains valid. Can be set only if the persistence cookie setting is enabled. Minimum value: 1

homePage Web address of the home page that a user is displayed when authentication vserver is bookmarked and used to login. Default value: "None"

show tm sessionParameter

Displays information about traffic session parameters.

Synopsis

show tm sessionParameter

Arguments

Output

name sessTimeout The session timeout, in minutes.

defaultAuthorizationAction The Authentication Action, e.g. allow or deny.

SSO Whether or not Single Sign-On is used for this session.

ssoCredential Use primary or secondary authentication credentials for single sign-on.

ssoDomain Domain to use for single sign-on.

kcdAccount Kerberos constrained delegation account name

httpOnlyCookie Allow only an HTTP session cookie, in which case the cookie cannot be accessed by scripts.

homePage Web address of the home page that a user is displayed when authentication vserver is bookmarked and used to login.

persistentCookie Use persistent SSO cookies for the traffic session. A persistent cookie remains on the user device and is sent with each HTTP request. The cookie becomes stale if the session ends.

persistentCookieValidity Integer specifying the number of minutes for which the persistent cookie remains valid. Can be set only if the persistence cookie setting is enabled.

tmsessionpolicyBindtype Indicates current bind type (Classic/Advanced) for TM session policy across all bind entities

tmsessionpolicyCount Count of TM session policies across all bind entities

unset tm sessionParameter

Resets the attributes of the specified traffic session parameters. Attributes for which a default value is available revert to their default values. Refer to the set tm sessionParameter command for descriptions of the parameters..Refer to the set tm sessionParameter command for meanings of the arguments.

Synopsis

unset tm sessionParameter

tm-sessionPolicy

The following operations can be performed on "tm-sessionPolicy":

unset| show| add| set| stat| rm|

unset tm sessionPolicy

Use this command to remove tm sessionPolicy settings.Refer to the set tm sessionPolicy command for meanings of the arguments.

Synopsis

unset tm sessionPolicy <name>

show tm sessionPolicy

Displays information about all the configured traffic management (TM) session policies, or displays detailed information about the specified TM session policy.

Synopsis

show tm sessionPolicy

Arguments

name Name of the session policy for which to display detailed information.

Output

stateflag rule Expression, against which traffic is evaluated. Both classic and advance expressions are supported in default partition but only advance expressions in non-default partition.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Action to be applied to connections that match this policy.

boundTo The entity name to which policy is bound

activePolicy priority bindPolicyType policyType builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

expressionType Type of policy (Classic/Advanced)

hits Number of hits.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

devno count

add tm sessionPolicy

Creates a traffic management (TM) session policy, which is applied after the user logs on to the AAA virtual server, to customize user sessions.

Synopsis

add tm sessionPolicy <name> <rule> <action>

Arguments

name Name for the session policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after a session policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

rule Expression, against which traffic is evaluated. Both classic and advance expressions are supported in default partition but only advance expressions in non-default partition.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Action to be applied to connections that match this policy.

set tm sessionPolicy

Modifies the rule or action of an existing traffic management (TM) session policy.

Synopsis

set tm sessionPolicy <name>

Arguments

name Name of the session policy to modify.

rule Expression, against which traffic is evaluated. Both classic and advance expressions are supported in default partition but only advance expressions in non-default partition.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Action to be applied to connections that match this policy.

stat tm sessionPolicy

Displays tm session statistics for all advanced tm session policies, or for only the specified policy.

Synopsis

stat tm sessionPolicy

Arguments

name Name of the advanced tmsession policy for which to display statistics. If no name is specified, statistics for all advanced tmsession polices are shown.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Policy undef hits (Undefhits) Number of undef hits on the policy

Example

stat tmsession policy

Related Commands

- stat tm trafficPolicy

rm tm sessionPolicy

Removes an existing traffic management (TM) session policy.

Synopsis

rm tm sessionPolicy <name>

Arguments

name Name of the session policy to remove.

tm-trafficAction

The following operations can be performed on "tm-trafficAction":

rm| unset| show| add| set|

rm tm trafficAction

Removes an existing traffic action.

Synopsis

rm tm trafficAction <name>

Arguments

name Name of the traffic action to remove.

unset tm trafficAction

Use this command to remove tm trafficAction settings.Refer to the set tm trafficAction command for meanings of the arguments.

Synopsis

unset tm trafficAction <name>

show tm trafficAction

Displays information about all configured traffic management (TM) traffic actions, or displays detailed information about the specified TM traffic action.

Synopsis

show tm trafficAction

Arguments

name Name of the traffic action for which to display detailed information.

Output

appTimeout The application timeout

SSO Whether or not Single Sign On is enabled.

formSSOAction Name of the configured form-based single sign-on profile.

stateflag persistentCookie Use persistent cookies for the traffic session. A persistent cookie remains on the user device and is sent with each HTTP request. The cookie becomes stale if the session ends.

InitiateLogout Whether Logout is initiated with this action

kcdAccount Kerberos contrained delegation account name

samlSSOProfile Profile to be used for doing SAML SSO to remote relying party

forcedTimeout Setting to start, stop or reset TM session force timer

forcedTimeoutVal Time interval, in minutes, for which force timer should be set.

userExpression expression that will be evaluated to obtain username for SingleSignOn

passwdExpression expression that will be evaluated to obtain password for SingleSignOn

devno count

add tm trafficAction

Creates a traffic action to set traffic characteristics at run time. You can create a traffic action for an application that is installed in the internal network (for example, an action that defines the destination IP address and destination port, and sets the amount of time a user can stay logged on to the application, such as 15 minutes).

Synopsis

add tm trafficAction <name> [-SSO (ON | OFF)]

Arguments

name Name for the traffic action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after a traffic action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

appTimeout Time interval, in minutes, of user inactivity after which the connection is closed. Minimum value: 1 Maximum value: 715827

SSO Use single sign-on for the resource that the user is accessing now.

Possible values: ON, OFF

formSSOAction Name of the configured form-based single sign-on profile.

persistentCookie Use persistent cookies for the traffic session. A persistent cookie remains on the user device and is sent with each HTTP request. The cookie becomes stale if the session ends.

Possible values: ON, OFF

InitiateLogout Initiate logout for the traffic management (TM) session if the policy evaluates to true. The session is then terminated after two minutes.

Possible values: ON, OFF

kcdAccount Kerberos constrained delegation account name Default value: "None"

samlSSOProfile Profile to be used for doing SAML SSO to remote relying party

forcedTimeout Setting to start, stop or reset TM session force timer

Possible values: START, STOP, RESET

forcedTimeoutVal Time interval, in minutes, for which force timer should be set.

userExpression expression that will be evaluated to obtain username for SingleSignOn Maximum value: 256

passwdExpression expression that will be evaluated to obtain password for SingleSignOn Maximum value: 256

set tm trafficAction

Modifies the specified parameters of an existing traffic action.

Synopsis

set tm trafficAction <name>

Arguments

name Name of the traffic action to modify.

appTimeout Time interval, in minutes, of user inactivity after which the connection is closed. Minimum value: 1 Maximum value: 715827

SSO Use single sign-on for the resource that the user is accessing now.

Possible values: ON, OFF

formSSOAction Name of the configured form-based single sign-on profile.

persistentCookie Use persistent cookies for the traffic session. A persistent cookie remains on the user device and is sent with each HTTP request. The cookie becomes stale if the session ends.

Possible values: ON, OFF

InitiateLogout Initiate logout for the traffic management (TM) session if the policy evaluates to true. The session is then terminated after two minutes.

Possible values: ON, OFF

kcdAccount Kerberos contrained delegation account name Default value: "None"

samlSSOProfile Profile to be used for doing SAML SSO to remote relying party

forcedTimeout Setting to start, stop or reset TM session force timer

Possible values: START, STOP, RESET

forcedTimeoutVal Time interval, in minutes, for which force timer should be set.

userExpression expression that will be evaluated to obtain username for SingleSignOn Maximum value: 256

passwdExpression expression that will be evaluated to obtain password for SingleSignOn Maximum value: 256

tm-trafficPolicy

The following operations can be performed on "tm-trafficPolicy":

set| rm| show| add| stat| unset|

set tm trafficPolicy

Modifies the specified parameters of an existing traffic policy.

Synopsis

set tm trafficPolicy <name>

Arguments

name Name of the traffic policy to modify.

rule Name of the Citrix ADC named expression, or an expression, that the policy uses to determine whether to apply certain action on the current traffic.

action Name of the action to apply to requests or connections that match this policy.

rm tm trafficPolicy

Removes an existing traffic policy.

Synopsis

rm tm trafficPolicy <name>

Arguments

name Name of the traffic policy to remove.

show tm trafficPolicy

Displays information about all configured traffic management (TM) traffic policies, or displays detailed information about the specified TM traffic policy.

Synopsis

show tm trafficPolicy

Arguments

name Name of the traffic policy for which to display detailed information.

Output

rule The rule used by the vpn traffic policy. Rules are combinations of Expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide

action The action to be performed when the rule is matched.

boundTo The entity name to which policy is bound

activePolicy priority hits Number of hits.

bindPolicyType vserverType stateflag devno count

add tm trafficPolicy

Adds a traffic policy to use for setting connection timeout, single sign-on, and initiating logout. The policy sets the characteristics of application traffic at run time.

Synopsis

add tm trafficPolicy <name> <rule> <action>

Arguments

name Name for the traffic policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

rule Name of the Citrix ADC named expression, or an expression, that the policy uses to determine whether to apply certain action on the current traffic.

action Name of the action to apply to requests or connections that match this policy.

stat tm trafficPolicy

Display Traffic Management traffic policy statistics.

Synopsis

stat tm trafficPolicy

Arguments

name The name of the TM traffic policy for which statistics will be displayed. If not given statistics are shown for all policies.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Example

stat tm trafficpolicy.

Related Commands

- stat tm sessionPolicy

unset tm trafficPolicy

Use this command to remove tm trafficPolicy settings.Refer to the set tm trafficPolicy command for meanings of the arguments.

Synopsis

unset tm trafficPolicy <name>

transform

transform-action

The following operations can be performed on "transform-action":

rm| unset| set| add| show|

rm transform action

Removes a URL Transformation action.

Synopsis

rm transform action <name>

Arguments

name Name of the action.

unset transform action

Use this command to remove transform action settings.Refer to the set transform action command for meanings of the arguments.

Synopsis

unset transform action <name>

set transform action

Modifies the settings of the specified URL Transformation action.

Synopsis

set transform action <name>

Arguments

name Name of the URL Transformation action to modify.

priority Positive integer specifying the priority of the action within the profile. A lower number specifies a higher priority. Must be unique within the list of actions bound to the profile. Policies are evaluated in the order of their priority numbers, and the first policy that matches is applied. Minimum value: 1 Maximum value: 2147483647

reqUrlFrom PCRE-format regular expression that describes the request URL pattern to be transformed.

reqUrlInto PCRE-format regular expression that describes the transformation to be performed on URLs that match the reqUrlFrom pattern.

resUrlFrom PCRE-format regular expression that describes the response URL pattern to be transformed.

resUrlInto PCRE-format regular expression that describes the transformation to be performed on URLs that match the resUrlFrom pattern.

cookieDomainFrom Pattern that matches the domain to be transformed in Set-Cookie headers.

cookieDomainInto PCRE-format regular expression that describes the transformation to be performed on cookie domains that match the cookieDomainFrom pattern. NOTE: The cookie domain to be transformed is extracted from the request.

state Enable or disable this action.

Possible values: ENABLED, DISABLED Default value: ENABLED

comment Any comments to preserve information about this URL Transformation action.

add transform action

Creates a URL Transformation action, which defines how a specific element in URLs in the request or response is to be modified. NOTE: In the URL Transformation feature (unlike all other Citrix ADC features), Â“profileÂ” and Â“actionÂ” are not synonymous but refer to distinct entities. You must create the profile first, and then the actions.

Synopsis

add transform action <name> <profileName> <priority>

Arguments

name Name for the URL transformation action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the URL Transformation action is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, Â“my transform actionÂ” or Â‘my transform action).

profileName Name of the URL Transformation profile with which to associate this action.

priority Positive integer specifying the priority of the action within the profile. A lower number specifies a higher priority. Must be unique within the list of actions bound to the profile. Policies are evaluated in the order of their priority numbers, and the first policy that matches is applied. Minimum value: 1 Maximum value: 2147483647

state Enable or disable this action.

Possible values: ENABLED, DISABLED Default value: ENABLED

show transform action

Displays a list of all URL Transformation actions currently assigned to the specified profile.

Synopsis

show transform action

Arguments

name Name of the profile.

Output

stateflag profileName Name of the URL Transformation profile with which to associate this action.

priority Positive integer specifying the priority of the action within the profile. A lower number specifies a higher priority. Must be unique within the list of actions bound to the profile. Policies are evaluated in the order of their priority numbers, and the first policy that matches is applied.

reqUrlFrom PCRE-format regular expression that describes the request URL pattern to be transformed.

reqUrlInto PCRE-format regular expression that describes the transformation to be performed on URLs that match the reqUrlFrom pattern.

resUrlFrom PCRE-format regular expression that describes the response URL pattern to be transformed.

resUrlInto PCRE-format regular expression that describes the transformation to be performed on URLs that match the resUrlFrom pattern.

cookieDomainFrom Pattern that matches the domain to be transformed in Set-Cookie headers.

cookieDomainInto PCRE-format regular expression that describes the transformation to be performed on cookie domains that match the cookieDomainFrom pattern. NOTE: The cookie domain to be transformed is extracted from the request.

continueMatching Continue transforming using the next rule in the list.

state Enable or disable this action.

comment Any comments to preserve information about this URL Transformation action.

devno count

Transform

The entities on which you can perform NetScaler CLI operations:

- transform-action
- transform-global
- transform-policy
- transform-policylabel
- transform-profile

transform-global

The following operations can be performed on "transform-global":

bind| show| unbind|

bind transform global

Activates the specified URL Transformation policy for all traffic received by this Citrix ADC. If you set policyName to a name that does not match an existing URL Transformation policy name, this command creates the policy, with the configuration that you specify.

Synopsis

bind transform global <policyName> <priority>

Arguments

policyName Name of the policy. If you want to create the policy as well as activate it, specify a name for the policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, Â“my transform policyÂ” or Â‘my transform policy).

priority Positive integer specifying the priority of the policy within the list of globally-bound URL transformation policies. A lower number specifies a higher priority. Must be unique within the list. Policies are evaluated in the order of their priorities, and the first policy that matches is applied. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Optional expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- A PCRE-compatible regular expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher priority number is evaluated next.

- If the expression evaluates to a number that is larger than the largest priority number, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.
- The expression evaluates to a priority number that is smaller than the current policy's priority number.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

type Bind point to which to bind the policy. Available settings function as follows:

- REQ_OVERRIDE. Request override. Binds the policy to the priority request queue.
- REQ_DEFAULT. Binds the policy to the default request queue.
- HTTPQUIC_REQ_OVERRIDE - Binds the policy to the HTTP_QUIC override request queue.
- HTTPQUIC_REQ_DEFAULT - Binds the policy to the HTTP_QUIC default request queue.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forwards the request or response to the specified virtual server or evaluates the specified policy label.

labelType Type of invocation. Available settings function as follows:

- reqvserver - Send the request to the specified request virtual server.
- resvserver - Send the response to the specified response virtual server.
- policylabel - Invoke the specified policy label.

Possible values: reqvserver, resvserver, policylabel

labelName Name of the policy label to invoke if the current policy evaluates to TRUE, the invoke parameter is set, and the label type is Policy Label.

Example

bind transform global pol9 9

show transform global

Displays the policies bound to the specified URL Transformation global bind point. If no bind point is specified, displays a list of all policies bound to URL Transformation global.

Synopsis

show transform global

Arguments

type Specifies the bind point to which to bind the policy. Available settings function as follows:

- REQ_OVERRIDE. Request override. Binds the policy to the priority request queue.
- REQ_DEFAULT. Binds the policy to the default request queue.
- HTTPQUIC_REQ_OVERRIDE - Binds the policy to the HTTP_QUIC override request queue.
- HTTPQUIC_REQ_DEFAULT - Binds the policy to the HTTP_QUIC default request queue.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT

Output

stateflag policyName Name of the transform policy.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forwards the request or response to the specified virtual server or evaluates the specified policy label.

labelType Type of invocation. Available settings function as follows:

- reqvserver - Send the request to the specified request virtual server.
- resvserver - Send the response to the specified response virtual server.
- policylabel - Invoke the specified policy label.

labelName Name of the policy label to invoke if the current policy evaluates to TRUE, the invoke parameter is set, and the label type is Policy Label.

flowType flowtype of the bound transform policy.

numpol The number of policies bound to the bindpoint.

flags globalBindType devno count

Example

show transform global

unbind transform global

Unbinds the specified URL Transformation policy from URL Transformation global.

Synopsis

unbind transform global <policyName>

Arguments

policyName The name of the policy to be unbound.

type The bindpoint from which the policy is to be unbound.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT

priority Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind transform global pol9

transform-policy

The following operations can be performed on "transform-policy":

add| set| show| stat| unset| rm| rename|

add transform policy

Creates a URL Transformation policy, which specifies the requests and responses to be transformed by the associated profile.

Synopsis

add transform policy <name> <rule> <profileName>

Arguments

name Name for the URL Transformation policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the URL Transformation policy is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, Â“my transform policyÂ” or Â‘my transform policy).

rule Expression, or name of a named expression, against which to evaluate traffic.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes blank spaces, the entire expression must be enclosed in double quotation marks.
- If the expression itself includes double quotation marks, you must escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

profileName Name of the URL Transformation profile to use to transform requests and responses that match the policy.

comment Any comments to preserve information about this URL Transformation policy.

logAction Log server to use to log connections that match this policy.

set transform policy

Modifies the specified parameters of a URL Transformation policy.

Synopsis

set transform policy <name>

Arguments

name Name of the policy to modify.

rule Expression, or name of a named expression, against which to evaluate traffic.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes blank spaces, the entire expression must be enclosed in double quotation marks.
- If the expression itself includes double quotation marks, you must escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

profileName Name of the URL Transformation profile to use to transform requests and responses that match the policy.

comment Any comments to preserve information about this URL Transformation policy.

logAction Log server to use to log connections that match this policy.

Example

set transform policy pol9 -rule "HTTP.REQ.HEADER(\\"header\\").CONTAINS(\\"qh2\\")"

show transform policy

Displays the current settings for the specified URL Transformation policy. If no policy name is specified, displays a list of all URL Transformation policies currently configured on the Citrix ADC.

Synopsis

show transform policy

Arguments

name Name of the URL Transformation policy.

Output

stateflag rule Expression, or name of a named expression, against which to evaluate traffic.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes blank spaces, the entire expression must be enclosed in double quotation marks.

- If the expression itself includes double quotation marks, you must escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

profileName Name of the URL Transformation profile to use to transform requests and responses that match the policy.

priority Specifies the priority of the policy.

hits Number of hits.

activePolicy Indicates whether policy is bound or not.

boundTo Location where policy is bound

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

comment Any comments to preserve information about this URL Transformation policy.

logAction Log server to use to log connections that match this policy.

bindPolicyType isDefault A value of true is returned if it is a default transform policy.

vserverType type builtin Flag to determine if Transform policy is built-in or not

feature The feature to be checked while applying this config

devno count

stat transform policy

Displays statistics for the specified URL Transformation policy. If no policy name is specified, displays abbreviated statistics for all URL Transformation policies currently configured on the Citrix ADC.

Synopsis

stat transform policy

Arguments

name Name of the policy.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Policy undef hits (Undefhits) Number of undef hits on the policy

Example

stat transform policy

Related Commands

- stat transform policylabel

unset transform policy

Removes the settings of an existing URL Transformation policy. Attributes for which a default value is available revert to their default values. See the set transform policy command for a description of the parameters..Refer to the set transform policy command for meanings of the arguments.

Synopsis

unset transform policy <name>

Example

unset transform policy pol9 -undefAction

rm transform policy

Removes the specified URL Transformation policy.

Synopsis

rm transform policy <name>

Arguments

name Name of the policy to remove.

Example

rm transform policy trans_pol

rename transform policy

Renames a URL Transformation policy.

Synopsis

rename transform policy <name>@ <newName>@

Arguments

name Existing name of the policy.

newName New name for the policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, Â“my transform policyÂ” or Â‘my transform policy).

Example

rename transform policy oldname newname

transform-policylabel

The following operations can be performed on "transform-policylabel":

rm| unbind| bind| stat| rename| add| show|

rm transform policylabel

Removes a URL Transformation policy label.

Synopsis

rm transform policylabel <labelName>

Arguments

labelName Name of the policy label to remove.

Example

rm transform policylabel trans_policylabel

unbind transform policylabel

Unbinds the specified URL Transformation policy from the specified policy label.

Synopsis

unbind transform policylabel <labelName> <policyName>

Arguments

labelName Name of the label from which to unbind the policy.

policyName Name of the label to which to bind the policy.

priority Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind transform policylabel trans_policylabel pol_1

bind transform policylabel

Binds the specified URL Transformation policy to the specified policy label.

Synopsis

bind transform policylabel <labelName> <policyName> <priority>

Arguments

labelName Name of the URL Transformation policy label to which to bind the policy.

policyName Name of the URL Transformation policy to bind to the policy label.

priority Positive integer specifying the priority of the policy within the policy label. A lower number specifies a higher priority. Must be unique within the list of policies bound to the label. Policies are evaluated in the order of their priority numbers, and the first policy that matches is applied. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Optional expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT.
- A PCRE-compatible regular expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher priority number is evaluated next.
- If the expression evaluates to a number that is larger than the largest priority number, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.
- The expression evaluates to a priority number that is smaller than the current policy's priority number.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

labelType Type of invocation. Available settings function as follows:

- reqvserver - Forward the request to the specified request virtual server.
- policylabel - Invoke the specified policy label.

Possible values: reqvserver, policylabel

labelName Name of the policy label to be invoke if the current policy evaluates to TRUE, the invoke parameter is set, and the label type is Policy Label.

Example

i)bind transform policylabel trans_policylabel pol_1 1 2 -invoke reqvserver CURRENT ii)bind transform policylabel trans_policylabel pol_2 2

stat transform policylabel

Displays statistics for the specified URL Transformation policy label. If no policy label name is provided, displays abbreviated statistics for all URL Transformation policy labels currently configured on the Citrix ADC.

Synopsis

stat transform policylabel

Arguments

labelName The name of the URL Transformation policy label.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy Label Hits (Hits) Number of times policy label was invoked.

rename transform policylabel

Renames a URL Transformation policy label.

Synopsis

rename transform policylabel <labelName>@ <newName>@

Arguments

labelName Current name of the policy label.

newName New name for the policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, Â“my transform policylabelÂ” or Â‘my transform policylabel).

Example

rename transform policylabel oldname newname

add transform policylabel

Creates a URL Transformation policy label. A policy label is a tool for evaluating a set of policies in a specified order. By using a policy label, you can configure the URL Transformation feature to choose the next policy, invoke a different policy label, or terminate policy evaluation completely by looking at whether the previous policy evaluated to TRUE or FALSE.

Synopsis

add transform policylabel <labelName> <policylabeltype>

Arguments

labelName Name for the policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the URL Transformation policy label is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, Â“my transform policylabelÂ” or Â‘my transform policylabel).

policylabeltype Types of transformations allowed by the policies bound to the label. For URL transformation, always http_req (HTTP Request).

Possible values: http_req, httpquic_req

Example

add transform policylabel trans_policylabel http_req

show transform policylabel

Displays the current settings for the specified URL Transformation policy label. If no policy label is specified, displays a list of all URL Transformation policy labels currently configured on the Citrix ADC.

Synopsis

show transform policylabel

Arguments

labelName Name for the policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the URL Transformation policy label is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, Â“my transform policylabelÂ” or Â‘my transform policylabel).

Output

stateflag policylabeltype Types of transformations allowed by the policies bound to the label. For URL transformation, always http_req (HTTP Request).

numpol Number of polices bound to label.

hits Number of times policy label was invoked.

policyName Name of the URL Transformation policy to bind to the policy label.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

labelType Type of invocation. Available settings function as follows:

- reqvserver - Forward the request to the specified request virtual server.
- policylabel - Invoke the specified policy label.

labelName Name of the policy label.

description Description of the policylabel

flags devno count

Example

i)show transform policylabel trans_policylabel ii)show transform policylabel

transform-profile

The following operations can be performed on "transform-profile":

show| add| set| rm| unset|

show transform profile

Displays the current settings for the specified URL Transformation profile. If no URL Transformation profile name is specified, displays a list of all URL Transformation profiles currently configured on the Citrix ADC.

Synopsis

show transform profile

Arguments

name Name of the profile.

Output

actionName URL Transformation action name.

stateflag type Type of transformation. Always URL for URL Transformation profiles.

RegexForFindingURLinJavaScript Patclass having regexes to find the URLs in JavaScript.

RegexForFindingURLinCSS Patclass having regexes to find the URLs in CSS.

RegexForFindingURLinXComponent Patclass having regexes to find the URLs in X-Component.

RegexForFindingURLinXML Patclass having regexes to find the URLs in XML.

additionalReqHeadersList Patclass having a list of additional request header names that should transformed.

additionalRespHeadersList Patclass having a list of additional response header names that should transformed.

onlyTransformAbsURLinBody In the HTTP body, transform only absolute URLs. Relative URLs are ignored.

comment Any comments to preserve information about this URL Transformation profile.

priority Priority of the Action within the Profile.

state Enabled flag.

profileName URL Transformation profile name.

reqUrlFrom Pattern of original request URLs. It corresponds to the way external users view the server, and acts as a source for request transformations.

reqUrlInto Pattern of transformed request URLs. It corresponds to internal addresses and indicates how they are created.

resUrlFrom Pattern of original response URLs. It corresponds to the way external users view the server, and acts as a source for response transformations.

resUrlInto Pattern of transformed response URLs. It corresponds to internal addresses and indicates how they are created.

cookieDomainFrom Pattern of the original domain in Set-Cookie headers.

cookieDomainInto Pattern of the transformed domain in Set-Cookie headers.

actionComment Comments.

devno count

add transform profile

Creates a URL transformation profile, which contains a list of actions that define how the URLs in a request or response are to be modified. NOTE: In the URL Transformation feature (unlike all other Citrix ADC features), Â“profileÂ” and Â“actionÂ” are not synonymous but refer to distinct entities. You must create the profile first, and then the actions.

Synopsis

add transform profile <name>

Arguments

name Name for the URL transformation profile. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the URL transformation profile is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, Â“my transform profileÂ” or Â‘my transform profileÂ’).

type Type of transformation. Always URL for URL Transformation profiles.

Possible values: URL

set transform profile

Modifies the settings of a URL Transformation profile.

Synopsis

set transform profile <name>

Arguments

name Name of the profile to be modified.

type Type of transformation. Always URL for URL Transformation profiles.

Possible values: URL

onlyTransformAbsURLinBody In the HTTP body, transform only absolute URLs. Relative URLs are ignored.

Possible values: ON, OFF

comment Any comments to preserve information about this URL Transformation profile.

rm transform profile

Removes a URL Transformation profile.

Synopsis

rm transform profile <name>

Arguments

name Name of the profile to remove.

unset transform profile

Use this command to remove transform profile settings.Refer to the set transform profile command for meanings of the arguments.

Synopsis

unset transform profile <name>

tunnel

Tunnel

The entities on which you can perform NetScaler CLI operations:

- tunnel-global
- tunnel-trafficPolicy

tunnel-global

The following operations can be performed on "tunnel-global":

show| unbind| bind|

show tunnel global

Displays globally active tunnel policies.

Synopsis

show tunnel global

Arguments

type Bind point to which the policy is bound.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

Output

policyName Policy name.

priority Priority.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

state Current state of the binding. If the binding is enabled, the policy is active.

numpol The number of policies bound to the bindpoint.

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

stateflag policyType Policy type (Classic/Advanced) to be bound.Used for display.

globalBindType devno count

Example

```
sh tunnel global
```

1. Policy Name: cmp_all_destport Priority: 0
2. Policy Name: local_sub_nocmp Priority: 500 Done

unbind tunnel global

Deactivates an active tunnel traffic policy.

Synopsis

unbind tunnel global <policyName>

Arguments

policyName Name of the tunnel traffic policy to unbind or deactivate.

type Bind point, specifying from where to unbind the policy. Applicable only to advanced (default-syntax) policies.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT, NONE

priority Priority of the policy to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

Globally active tunnel policies can be seen using command:

```
show tunnel global 1 Globally Active Tunnel Policies:
```

1. Policy Name: cmp_all_destport Priority: 0 Done

The globally active tunnel traffic policy can be deactivated on the Citrix ADC system by issuing the command: unbind tunnel global cmp_all_destport

bind tunnel global

Activates an existing tunnel traffic policy globally.

Synopsis

bind tunnel global (<policyName>)

Arguments

policyName Name of the tunnel traffic policy to activate or bind.

priority Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Minimum value: 0 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy l abel performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.

- The expression evaluates to a priority number that is smaller than the current policy's priority number.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression ev aluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

state Current state of the binding. If the binding is enabled, the policy is active.

Possible values: ENABLED, DISABLED Default value: ENABLED

type Global bind point, specifying where to bind the policy. This is relevant for advanced (default-syntax) policies only.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT, NONE Default value: NONE

Example

add tunnel trafficpolicy cmp_all_destport "REQ.TCP.DESTPORT == 0-65535" GZIP

After creating above tunnel policy, it can be activated by binding it globally: bind tunnel global cmp_all_destport

After binding cmp_all_destport compression policy globally, the policy gets activated and the Citrix ADC will compress all TCP traffic accessed through ssl-vpn tunnel.

Globally active tunnel policies can be seen using command:

```
show tunnel global 1 Globally Active Tunnel Policies:
```

1. Policy Name: cmp_all_destport Priority: 0 Done

tunnel-trafficPolicy

The following operations can be performed on "tunnel-trafficPolicy":

add| rename| rm| unset| set| show| stat|

add tunnel trafficPolicy

Creates a tunnel traffic policy. A tunnel traffic policy defines the type of compression to be used for the tunneled traffic.

Synopsis

add tunnel trafficPolicy <name> <rule> <action>

Arguments

name Name for the tunnel traffic policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy)'.

rule Expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI:

- If the expression includes blank spaces, the entire expression must be enclosed in double quotation marks.
- If the expression itself includes double quotation marks, you must escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the built-in compression action to associate with the policy.

comment Any comments to preserve information about this policy.

logAction Name of the messagelog action to use for requests that match this policy.

Example

Example 1: add tunnel trafficpolicy cmp_all_destport "REQ.TCP.DESTPORT == 0-65535" GZIP

After creating above tunnel policy, it can be activated by binding it globally: bind tunnel global cmp_all_destport

The policy is evaluated for all traffic flowing through the ssl-vpn tunnel, and compresses traffic for all TCP application ports.

Example 2: The following tunnel policy disables compression for all access from a specific subnet: add tunnel trafficpolicy local_sub_nocmp "SOURCEIP == 10.1.1.0 -netmask 255.255.255.0" NOCOMPRESS bind tunnel global local_sub_nocmp

rename tunnel trafficPolicy

Renames a tunnel traffic policy.

Synopsis

rename tunnel trafficPolicy <name>@ <newName>@

Arguments

name Existing name of the policy.

newName New name for the tunnel traffic policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), e quals (=), and hyphen (-) characters. Choose a name that reflects the function that the policy performs.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my tunnel policy" or 'my tunnel policy').

Example

rename tunnel trafficPolicy oldname newname

rm tunnel trafficPolicy

Removes a tunnel traffic policy.

Synopsis

rm tunnel trafficPolicy <name>

Arguments

name Name of the tunnel traffic policy to remove.

Example

rm tunnel trafficpolicy tunnel_policy_name The "show tunnel trafficpolicy" command shows all tunnel policies that are currently defined.

unset tunnel trafficPolicy

Use this command to remove tunnel trafficPolicy settings.Refer to the set tunnel trafficPolicy command for meanings of the arguments.

Synopsis

unset tunnel trafficPolicy <name>

set tunnel trafficPolicy

Modifies the specified parameters of an existing tunnel traffic policy.

Synopsis

set tunnel trafficPolicy <name>

Arguments

name Name of the tunnel traffic policy to modify.

rule Expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI:

- If the expression includes blank spaces, the entire expression must be enclosed in double quotation marks.
- If the expression itself includes double quotation marks, you must escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the built-in compression action to associate with the policy.

comment Any comments to preserve information about this policy.

logAction Name of the messagelog action to use for requests that match this policy.

Example

add tunnel trafficpolicy cmp_all_destport "REQ.TCP.DESTPORT == 0-65535" GZIP set tunnel trafficpolicy cmp_all_destport -action NOCOMPRESS

Above 'set' command changes action for policy cmp_all_destport from GZIP to NOCOMPRESS

show tunnel trafficPolicy

Displays information about all the configured tunnel traffic policies, or displays detailed information about the specified tunnel traffic policy.

Synopsis

show tunnel trafficPolicy show tunnel trafficPolicy stats - alias for 'stat tunnel trafficPolicy'

Arguments

name Name of the tunnel traffic policy for which to show detailed information.

Output

stateflag expressionType Type of policy (Classic/Advanced)

rule Expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI:

- If the expression includes blank spaces, the entire expression must be enclosed in double quotation marks.
- If the expression itself includes double quotation marks, you must escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the built-in compression action to associate with the policy.

hits No of hits.

undefHits Number of policy UNDEF hits.

txbytes Number of bytes transmitted.

rxbytes Number of bytes received.

clientTTLB Total client TTLB value.

clientTransactions Number of client transactions.

serverTTLB Total server TTLB value.

serverTransactions Number of server transactions.

piHits Number of hits.

piTxBytes Number of bytes transmitted.

piRxBytes Number of bytes received.

piCltTTLB Total client TTLB value.

piCltTransactions Number of client transactions.

piSvrTTLB Total server TTLB value.

piSvrTransactions Number of server transactions.

comment Any comments to preserve information about this policy.

logAction Name of the messagelog action to use for requests that match this policy.

boundTo The entity name to which policy is bound

activePolicy priority gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

flags bindPolicyType isDefault A value of true is returned if it is a default tunnelpolicy.

policyType builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

devno count

Example

> show tunnel trafficpolicy 2 Tunnel policies:

1. Name: local_sub_nocmp Rule: SOURCEIP == 10.1.1.0 -netmask 255.255.255.0 Action: NOCOMPRESS Hits: 3
2. Name: cmp_all Rule: REQ.TCP.DESTPORT == 0-65535 Action: GZIP Hits: 57125 Bytes In:...796160 Bytes Out:... 197730 Bandwidth saving...75.16% Ratio 4.03:1 Done

stat tunnel trafficPolicy

Displays statistics for all advanced tunnel traffic policies, or for only the specified policy.

Synopsis

stat tunnel trafficPolicy

Arguments

name Name of the advanced tunnel traffic policy.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Policy undef hits (Undefhits) Number of undef hits on the policy

Example

stat tunnel trafficpolicy

ulfd

Ulfd

The entities on which you can perform NetScaler CLI operations:

- ulfd-server

ulfd-server

The following operations can be performed on "ulfd-server":

rm| add| show|

rm ulfd server

Removes a ulfd server from the Citrix ADC. NOTE: This command is deprecated.Deprecated in favour of appflow collector command

Synopsis

Arguments

loggerip IP address of the server where ulfd service is running.

add ulfd server

Adds a ulfd server to the Citrix ADC. NOTE: This command is deprecated.Deprecated in favour of appflow collector command

Synopsis

Arguments

loggerip IP address of the server where ulfd service is running.

show ulfd server

Displays ulfd server ip address and server state. NOTE: This command is deprecated.Deprecated in favour of appflow collector command

Synopsis

Arguments

loggerip IP address of the server where ulfd service is running.

Output

state ULFD server state.

devno count stateflag

urlfiltering

urlfiltering-Categories

The following operations can be performed on "urlfiltering-Categories":

show urlfiltering Categories

Displays a list of all URL Filtering Categories.

Synopsis

show urlfiltering Categories

Arguments

Group URL Filtering SDK Category per Group. Default value: NS_S_URLFILT_GROUP_DEFAULT

Output

Categories URL Filtering SDK Categories.

Example

show urlfiltering Categories

urlfiltering-Categorization

The following operations can be performed on "urlfiltering-Categorization":

clear| show| add|

clear urlfiltering Categorization

Clears the list of urls placed for categorization

Synopsis

clear urlfiltering Categorization

Example

clear urlfiltering Categorization

show urlfiltering Categorization

Displays categorization results for all added URLs

Synopsis

show urlfiltering Categorization

Arguments

Output

Categorization NetStar SDK URL Categorization result for a specific url.

Url Url given for categorization.

devno count stateflag

Example

show urlfiltering Categorization

add urlfiltering Categorization

Adds a url for categorization

Synopsis

add urlfiltering Categorization -Url <string>

Arguments

Url Url given for categorization. Default value: NS_S_URLFILT_URL_DEFAULT

Example

add urlfiltering Categorization -url www.google.com

urlfiltering-CategoryGroups

The following operations can be performed on "urlfiltering-CategoryGroups":

show urlfiltering CategoryGroups

Displays a list of all URL Filtering Category Groups.

Synopsis

show urlfiltering CategoryGroups

Arguments

Output

CategoryGroups URL Filtering SDK Category Groups.

Example

show urlfiltering CategoryGroups

Urlfiltering

The entities on which you can perform NetScaler CLI operations:

- urlfiltering-Categories
- urlfiltering-Categorization
- urlfiltering-CategoryGroups
- urlfiltering-parameter

urlfiltering-parameter

The following operations can be performed on "urlfiltering-parameter":

set| unset| show|

set urlfiltering parameter

Modifies the specified URL Filtering parameters.

Synopsis

set urlfiltering parameter

Arguments

HoursBetweenDBUpdates URL Filtering hours between DB updates. Default value: NS_S_URLFILT_HOURS_BETWEENDB_UPDATES_DEFAULT Minimum value: 0 Maximum value: 720

TimeOfDayToUpdateDB URL Filtering time of day to update DB. Default value: NS_S_URLFILT_TIME_OFDAY_TO_UPDATE_DB_DEFAULT

LocalDatabaseThreads URL Filtering Local DB number of threads. Default value: NS_S_URLFILT_LOCAL_DB_THREADS Minimum value: 1 Maximum value: 4

CloudHost URL Filtering Cloud host. Default value: NS_S_URLFILT_CLOUD_HOST_DEFAULT

SeedDBPath URL Filtering Seed DB path. Default value: NS_S_URLFILT_SEEDDB_PATH_DEFAULT

Example

set urlfiltering parameter -urlfilt_hours_betweenDB_updates 20)

unset urlfiltering parameter

Use this command to remove urlfiltering parameter settings.Refer to the set urlfiltering parameter command for meanings of the arguments.

Synopsis

unset urlfiltering parameter

show urlfiltering parameter

Displays the URL Filtering parameters.

Synopsis

show urlfiltering parameter

Arguments

Output

HoursBetweenDBUpdates URL Filtering hours between DB updates.

TimeOfDayToUpdateDB URL Filtering time of day to update DB.

MaxNumberOfCloudThreads URL Filtering hours between DB updates.

CloudKeepAliveTimeout URL Filtering Cloud keep alive timeout in msec.

CloudServerConnectTimeout URL Filtering Cloud server connect timeout in msec.

CloudDBLookupTimeout URL Filtering CloudDB send/receive timeout in msec.

ProxyHostIp URL Filtering Cloud Proxy HostIp.

ProxyPort URL Filtering Cloud Proxy Port.

ProxyUsername URL Filtering Cloud Proxy Username.

ProxyPassword URL Filtering Cloud Proxy Password.

SDKLicenseKey URL Filtering SDK License Key.

seedDBSizeLevel URL Filtering Seed DB Size Level to get downloaded.

LocalDatabaseThreads URL Filtering Local DB number of threads.

CloudHost URL Filtering Cloud host.

SeedDBPath URL Filtering Seed DB path.

Example

show urlfiltering parameter

user

User

The entities on which you can perform NetScaler CLI operations:

- user-protocol
- user-vserver

user-protocol

The following operations can be performed on "user-protocol":

set| show| add| unset| rm|

set user protocol

Modifies the specified parameters of an user protocol.

Synopsis

set user protocol <name> -comment <string>

Arguments

name Unique name for the user protocol. Not case sensitive. Must begin with an ASCII letter or underscore (_) character, and must consist only of ASCII alphanumeric or underscore characters.

comment Any comments associated with the protocol.

show user protocol

Displays information about the available user protocols.

Synopsis

show user protocol

Arguments

name Unique name for the user protocol. Not case sensitive. Must begin with an ASCII letter or underscore (_) character, and must consist only of ASCII alphanumeric or underscore characters.

Output

transport Transport layer's protocol.

extension Name of the extension to add parsing and runtime handling of the protocol packets.

comment Any comments associated with the protocol.

stateflag devno count

add user protocol

Add the user protocol Example: add user protocol MQTT -transporttype TCP -extension mqtt_logic

Synopsis

add user protocol <name> -transport (TCP | SSL) -extension <string>

Arguments

name Unique name for the user protocol. Not case sensitive. Must begin with an ASCII letter or underscore (_) character, and must consist only of ASCII alphanumeric or underscore characters.

transport Transport layer's protocol.

Possible values: TCP, SSL

extension Name of the extension to add parsing and runtime handling of the protocol packets.

comment Any comments associated with the protocol.

unset user protocol

Use this command to remove user protocol settings.Refer to the set user protocol command for meanings of the arguments.

Synopsis

unset user protocol <name> -comment

rm user protocol

Removes an user protocol.

Synopsis

rm user protocol <name>

Arguments

name Unique name for the user protocol. Not case sensitive. Must begin with an ASCII letter or underscore (_) character, and must consist only of ASCII alphanumeric or underscore characters.

user-vserver

The following operations can be performed on "user-vserver":

unset| disable| rm| set| show| stat| add| enable|

unset user vserver

Use this command to remove user vserver settings.Refer to the set user vserver command for meanings of the arguments.

Synopsis

unset user vserver <name>

disable user vserver

Disables an user virtual server.

Synopsis

disable user vserver <name>@

Arguments

name Name of the user virtual server to be disabled.

Example

disable user vserver user_vip

rm user vserver

Removes an user defined virtual server from the Citrix ADC.

Synopsis

rm user vserver <name>

Arguments

name Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver').

set user vserver

Modifies the specified parameters of an user defined virtual server.

Synopsis

set user vserver <name>

Arguments

name Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver').

IPAddress IPv4 or IPv6 address to assign to the virtual server.

defaultLB Name of the default Load Balancing virtual server used for load balancing of services. The protocol type of default Load Balancing virtual server should be a user type.

params Any comments associated with the protocol.

comment Any comments that you might want to associate with the virtual server.

show user vserver

Displays information about the user defined virtual server.

Synopsis

show user vserver

Arguments

name Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver').

Output

userProtocol User protocol uesd by the service.

IPAddress IPv4 or IPv6 address to assign to the virtual server.

port Port number for the virtual server.

defaultLB Name of the default Load Balancing virtual server used for load balancing of services. The protocol type of default Load Balancing virtual server should be a user type.

params Any comments associated with the protocol.

comment Any comments that you might want to associate with the virtual server.

stateflag state Current user vserver state.

value SSL status.

stateChangeTimeSec Time when last state change happened. Seconds part.

stateChangeTimemSec Time at which last state change happened. Milliseconds part.

ticksSinceLastStateChange Time in 10 millisecond ticks since the last state change.

state Initial state of the user vserver.

noDefaultBindings to determine if the configuration will have default ssl CIPHER and ECC curve bindings

devno count

stat user vserver

Displays the statistical data collected for an user defined load balancing virtual server.

Synopsis

stat user vserver [-sortBy Hits]

Arguments

name Name of the user defined virtual server. If no name is provided, statistical data of all configured user defined virtual servers is displayed.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

sortBy use this argument to sort by specific key

Possible values: Hits

sortOrder use this argument to specify sort order

Possible values: ascending, descending Default value: SORT_DESCENDING

Output

count devno stateflag

Counters

Current Client Est connections (ClntEstConn) Number of client connections in ESTABLISHED state.

total INACTIVE services (inactSvcs) number of INACTIVE services bound to a vserver

Vserver Health (Health) Health of the vserver. This gives percentage of UP services bound to this vserver.

Vserver IP address (vsvrIP) IP address of the vserver

Port (port) The port on which the service is running.

Vserver protocol name (Protocol) Protocol associated with the vserver

State Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)

total ACTIVE services (actSvcs) number of ACTIVE services bound to a vserver

Vserver hits (Hits) Total vserver hits

Requests (Req) Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Responses (Rsp) Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Request bytes (Reqb) Total number of request bytes received on this service or virtual server.

Response bytes (Rspb) Number of response bytes received by this service or virtual server.

Total Packets rcvd (PktRx) Total number of packets received by this service or virtual server.

Total Packets sent (PktTx) Total number of packets sent.

Current client connections (ClntConn) Number of current client connections.

Current server connections (SvrConn) Number of current connections to the actual servers behind the virtual server.

Invalid Request/Response (IvldReqRsp) Number invalid requests/responses on this vserver

Invalid Request/Response Dropped (IvldReqRspDrp) Number invalid requests/responses dropped on this vserver

Current Server Est connections (SvrEstConn) Number of server connections in ESTABLISHED state.

add user vserver

Creates an user defined load balancing virtual server. Example: add user protocol MQTT -transporttype TCP -extension mqtt_logic

Synopsis

add user vserver <name>@ <userProtocol> <IPAddress>@ <port> -defaultLB <string>

Arguments

name Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver').

userProtocol User protocol uesd by the service.

IPAddress IPv4 or IPv6 address to assign to the virtual server.

port Port number for the virtual server.

defaultLB Name of the default Load Balancing virtual server used for load balancing of services. The protocol type of default Load Balancing virtual server should be a user type.

params Any comments associated with the protocol.

comment Any comments that you might want to associate with the virtual server.

state Initial state of the user vserver.

Possible values: ENABLED, DISABLED Default value: ENABLED

enable user vserver

Enables an user virtual server.

Synopsis

enable user vserver <name>@

Arguments

name Name of the user virtual server to enable. Note: Virtual servers, when added, are enabled by default.

Example

enable user vserver user_vip

utility

callhome

The following operations can be performed on "callhome":

set| show| unset|

set callhome

Sets CallHome parameters

Synopsis

set callhome

Arguments

mode CallHome mode of operation

Possible values: Default, CSP Default value: Default

emailAddress Email address of the contact administrator.

hbCustomInterval Interval (in days) between CallHome heartbeats Default value: 7 Minimum value: 1 Maximum value: 30

proxyMode Enables or disables the proxy mode. The proxy server can be set by either specifying the IP address of the server or the name of the service representing the proxy server.

Possible values: YES, NO Default value: NO

IPAddress IP address of the proxy server.

proxyAuthService Name of the service that represents the proxy server.

port HTTP port on the Proxy server. This is a mandatory parameter for both IP address and service name based configuration. Minimum value: 1

Example

set callhome -mode default -emailAddress abc@xyz.com -proxyMode YES -proxyauthService callhome_proxy -port 80 -hbCustomInterval 6

show callhome

Displays the CallHome configuration and trigger event details.

Synopsis

show callhome

Arguments

Output

mode CallHome mode of operation

emailAddress Email address of the contact administrator.

hbCustomInterval Interval (in days) between CallHome heartbeats

proxyMode Enables or disables the proxy mode. The proxy server can be set by either specifying the IP address of the server or the name of the service representing the proxy server.

IPAddress IP address of the proxy server.

port HTTP port on the Proxy server. This is a mandatory parameter for both IP address and service name based configuration.

proxyAuthService Name of the service that represents the proxy server.

sslcardfirstfailure First occurrence SSL card failure.

sslcardlatestfailure Latest occurrence SSL card failure.

powfirstfail First occurrence power supply unit failure.

powlatestfailure Latest occurrence power supply unit failure.

HDDfirstfail First occurrence hard disk drive failure.

HDDlatestfailure Latest occurrence hard disk drive failure.

FLASHfirstfail First occurrence compact flash failure.

FLASHlatestfailure Latest occurrence compact flush failure.

RLfirstHighDrop First occurence of high rate limit drops

RLlatestHighDrop Latest occurence of high rate limit drops

restartLatestfail Latest occurrence warm restart failure.

memthreFirstAnomaly First occurrence of memory anomaly.

memthreLatestAnomaly Latest occurrence of memory anomaly.

callhomestatus Callhome feature enabled/disable, register with upload server successful/failed

anomalyDetection Enables or disables anomaly detection.

Example

show callhome Mode: Default E-mail address configured:xxx@yahoo.com Heartbeat Custom Interval(days): 20

Trigger event State First occurrence Latest occurrence

1. Compact flash errors Enabled ....
2. Hard disk drive errors Enabled ....
3. Power supply unit failure Enabled 27 Aug 2010 18:22:47 28 Aug 2010 18:22:47
4. SSL card failure Enabled 25 Aug 2010 18:22:47 26 Aug 2010 18:22:47
5. Warm restart Enabled N/A ..

unset callhome

Use this command to remove callhome settings.Refer to the set callhome command for meanings of the arguments.

Synopsis

unset callhome

grep

The following operations can be performed on "grep":

grep

Searches files or output for lines containing a match to the specified . By default, grep prints the matching lines.

Synopsis

grep <pattern>

Arguments

c Suppress normal output. Instead print a count of matching lines. With the -v option, count non-matching lines.

E Interpret <pattern> as an extended regular expression.

i Ignore case distinctions.

v Invert the sense of matching, to select non-matching lines.

w Select only those lines containing matches that form whole words.

x Select only those matches that exactly match the whole line.

pattern The pattern (regular expression or text string) for which to search.

Example

show ns info | grep off -i

install

The following operations can be performed on "install":

install

Installs a version of Citrix ADC software on the system.

Synopsis

install <url>

Arguments

url Url for the build file. Must be in the following formats: http://:@host/path/to/file https://:@host/path/to/file sftp://:@host/path/to/file scp://:@host/path/to/file ftp://:@host/path/to/file file://path/to/file

y Do not prompt for yes/no before rebooting.

L Use this flag to enable callhome.

A Use this flag to enable Citrix ADM Service Connect. This feature helps you discover your Citrix ADC instances effortlessly on Citrix ADM service and get insights and curated machine learning based recommendations for applications and Citrix ADC infrastructure. This feature lets the Citrix ADC instance automatically send system, usage and telemetry data to Citrix ADM service. View here to learn more about this feature. Use of this feature is subject to the Citrix End User ServiceAgreement. View here .

enhancedUpgrade Use this flag for upgrading from/to enhancement mode.

resizeSwapVar Use this flag to change swap size on ONLY 64bit nCore/MCNS/VMPE systems NON-VPX systems.

async Use this flag to return the install id when the nitro api request is sent. The id can be used later to track the installation progress via show ns job <id> command. For the cli request of install the flag is by default set as false as the installation progress details can be tracked via cli

Output

Id Job Id for install process

Example

install http://host.netscaler.com/ns-6.0-41.2.tgz

ping

The following operations can be performed on "ping":

ping

Invokes the UNIX ping command. The hostName parameter must be used if the name is in the /etc/hosts file directory or is otherwise known in DNS.

Synopsis

ping <hostname>

Arguments

c Number of packets to send. The default value is infinite. For Nitro API, defalut value is taken as 5. Minimum value: 1 Maximum value: 65535

i Waiting time, in seconds. The default value is 1 second. Minimum value: 0 Maximum value: 65535

I Network interface on which to ping, if you have multiple interfaces.

n Numeric output only. No name resolution.

p Pattern to fill in packets. Can be up to 16 bytes, useful for diagnosing data-dependent problems.

q Quiet output. Only the summary is printed. For Nitro API, this flag is set by default.

s Data size, in bytes. The default value is 56. Minimum value: 0 Maximum value: 65507

S Source IP address to be used in the outgoing query packets. If the IP addrESS does not belongs to this appliance, an error is returned and nothing is sent.

T Traffic Domain Id Minimum value: 1 Maximum value: 4094

t Time-out, in seconds, before ping exits. Minimum value: 1 Maximum value: 3600

hostName Address of host to ping.

Output

response

Example

ping -p ff -c 4 10.102.4.107

ping6

The following operations can be performed on "ping6":

ping6

Invokes the UNIX ping6 command. The hostName parameter must be used if the name is in the /etc/hosts file directory or is otherwise known in DNS.

Synopsis

ping6 Hostname

Arguments

b Set socket buffer size. If used, should be used with roughly +100 then the datalen (-s option). The default value is 8192. Minimum value: 132 Maximum value: 131071

c Number of packets to send. The default value is infinite. For Nitro API, defalut value is taken as 5. Minimum value: 1 Maximum value: 65535

i Waiting time, in seconds. The default value is 1 second. Minimum value: 0 Maximum value: 65535

I Network interface on which to ping, if you have multiple interfaces.

m By default, ping6 asks the kernel to fragment packets to fit into the minimum IPv6 MTU.The -m option will suppress the behavior for unicast packets.

n Numeric output only. No name resolution.

p Pattern to fill in packets. Can be up to 16 bytes, useful for diagnosing data-dependent problems.

q Quiet output. Only summary is printed. For Nitro API, this flag is set by default

s Data size, in bytes. The default value is 32. Minimum value: 0 Maximum value: 65527

V VLAN ID for link local address. Minimum value: 1 Maximum value: 4094

S Source IP address to be used in the outgoing query packets.

T Traffic Domain Id Minimum value: 1 Maximum value: 4094

hostName Address of host to ping.

Output

response

Example

ping6 -p ff -I 1/1 -c 4 2002::1

raid

The following operations can be performed on "raid":

show raid

Provides status of raid

Synopsis

show raid

Example

status raid

scp

The following operations can be performed on "scp":

scp

Securely copies data from one computer to another, in SSH protocol.

Synopsis

scp <sourceString> <destString>

Arguments

r Recursively copy subdirectories.

C Enable compression.

q Quiet output. Disable the progress meter.

sourceString Source user, host, and file path, specified as <user>@<host>:<path_to_copy_from>. The user and host parts are optional.

destString Destination user, host, and file path, specified as <user>@<host>:<path_to_copy_to>. The user and host parts are optional.

Example

scp /nsconfig/ns.conf nsroot@10.102.4.107:/nsconfig/

shell

The following operations can be performed on "shell":

shell

Exits to the FreeBSD command prompt. Press Control + D or type exit to return to the Citrix ADC command prompt. Note: The shell can be accessed only by users who have write access to the Citrix ADC.

Synopsis

shell

Arguments

command Shell command(s) to be invoked.

Example

```
shell
```

ps

| grep nscli 485 p0 S 0:01.12 -nscli (nscli) 590 p0 S+ 0:00.00 grep nscli

\^D Done

```
shell ps -aux |grep nscli 485 p0 S 0:01.12 -nscli (nscli) 590 p0 S+ 0:00.00 grep nscli
```

techsupport

The following operations can be performed on "techsupport":

show techsupport

Generates a gzipped tar archive of system configuration data and statistics. To minimize archive file size newnslog collection is restricted to 500mb, 6 files, or 7 days, whichever occurs first. If the files under /var/log/ grow bigger, the entire file copy is avoided and few lines from those log files

are copied. If older data is needed, it may require manual collection. The archive should be submitted to Citrix Technical Support for further analysis and is available at the following path:

/var/tmp/support/support.tgz.

The above path is a symlink to the most recent collector for easy access. The full filename varies based on deployment topology but generally follows a format similar to:

collector___.tgz.

The output path and filename are displayed to the user when the command is executed.

Synopsis

show techsupport [-upload]

Arguments

scope Use this option to gather data on the present node, all cluster nodes, or for the specified partitions. The CLUSTER scope generates smaller abbreviated archives for all nodes. The PARTITION scope collects the admin partition in addition to those specified. The partitionName option is only required for the PARTITION scope.

Possible values: NODE, CLUSTER, PARTITION Default value: NODE

partitionName Name of the partition

upload Securely upload the collector archive to Citrix Technical Support using SSL. MyCitrix credentials will be required. If used with the -file option, no new collector archive is generated. Instead, the specified archive is uploaded. Note that the upload operation time depends on the size of the archive file, and the connection bandwidth.

proxy Specifies the proxy server to be used when uploading a collector archive. Use this parameter if the Citrix ADC does not have direct internet connectivity. The basic format of the proxy string is: "proxy_IP:<proxy_port>" (without quotes). If the proxy requires authentication the format is: "username:password@proxy_IP:<proxy_port>"

casenumber Specifies the associated case or service request number if it has already been opened with Citrix Technical Support.

file Specifies the name (with full path) of the collector archive file to be uploaded. If this is specified, no new collector archive is generated.

description Provides a text description for the the upload, and can be used for logging purposes.

userName Specifies My Citrix user name, which is used to login to Citrix upload server

password Specifies My Citrix password, which is used to login to Citrix upload server

time Specifies the time in common log format, ie. DD/MMM/YYYY:HH:MM:SS, to be used for locating the newnslog file. With this option at most four newnslog log files are collected. First is the newnslog file, spanning the given time. Second is the one, created just prior to the first (if it exists). Third is the one, created just later than the first (if it exists). And the fourth is the latest newnslog directory. In case, the scope is cluster, then second and third type is skipped on all nodes.

adss Option for collecting showtechsupport bundle on ADSS cluster/node.

nodes Use this option to collect showtechsupport bundle only from the nodes given as a list to this option. If -file option is used, it will collect the files from the given nodes back to the cco and will upload the compressed folder containing the files from there. Minimum value: 0 Maximum value: 255

Output

response Output as text printed to console and syslog at NOTICE level.

serverName

Example

show techsupport show techsupport -upload -case 71234567 show techsupport -scope CLUSTER

traceroute

The following operations can be performed on "traceroute":

traceroute

Invokes the UNIX traceroute command. This command attempts to track the route that the packets follow to reach the destination host.

Synopsis

traceroute -P <protocol> <host>

Arguments

S Print a summary of how many probes were not answered for each hop.

n Print hop addresses numerically instead of symbolically and numerically.

r Bypass normal routing tables and send directly to a host on an attached network. If the host is not on a directly attached network, an error is returned.

v Verbose output. List received ICMP packets other than TIME_EXCEEDED and UNREACHABLE.

M Minimum TTL value used in outgoing probe packets. Default value: 1 Minimum value: 1 Maximum value: 255

m Maximum TTL value used in outgoing probe packets. For Nitro API, default value is taken as 10. Default value: 64 Minimum value: 1 Maximum value: 255

P Send packets of specified IP protocol. The currently supported protocols are UDP and ICMP.

p Base port number used in probes. Default value: 33434 Minimum value: 1 Maximum value: 65535

q Number of queries per hop. For Nitro API, defalut value is taken as 1. Default value: 3 Minimum value: 1 Maximum value: 65535

s Source IP address to use in the outgoing query packets. If the IP address does not belong to this appliance, an error is returned and nothing is sent.

T Traffic Domain Id Minimum value: 1 Maximum value: 4094

t Type-of-service in query packets. Maximum value: 255

w Time (in seconds) to wait for a response to a query. For Nitro API, defalut value is set to 3. Default value: 5 Minimum value: 2 Maximum value: 86399

host Destination host IP address or name.

packetlen Length (in bytes) of the query packets. Default value: 44 Minimum value: 44 Maximum value: 32768

Output

response

Example

traceroute 10.102.4.107

traceroute6

The following operations can be performed on "traceroute6":

traceroute6

Invokes the UNIX traceroute6 command. Traceroute6 attempts to track the route that the packets follow to reach the destination host.

Synopsis

traceroute6 <target>

Arguments

n Print hop addresses numerically rather than symbolically and numerically.

I Use ICMP ECHO for probes.

r Bypass normal routing tables and send directly to a host on an attached network. If the host is not on a directly attached network, an error is returned.

v Verbose output. List received ICMP packets other than TIME_EXCEEDED and UNREACHABLE.

m Maximum hop value for outgoing probe packets. For Nitro API, default value is taken as 10. Default value: 64 Minimum value: 1 Maximum value: 255

p Base port number used in probes. Default value: 33434 Minimum value: 1 Maximum value: 65535

q Number of probes per hop. For Nitro API, default value is taken as 1. Default value: 3 Minimum value: 1 Maximum value: 65535

s Source IP address to use in the outgoing query packets. If the IP address does not belong to this appliance, an error is returned and nothing is sent.

T Traffic Domain Id Minimum value: 1 Maximum value: 4094

w Time (in seconds) to wait for a response to a query. For Nitro API, defalut value is set to 3. Default value: 5 Minimum value: 2 Maximum value: 86399

host Destination host IP address or name.

packetlen Length (in bytes) of the query packets. Default value: 44 Minimum value: 44 Maximum value: 32768

Output

response

Example

traceroute6 2002::7

Utility

The entities on which you can perform NetScaler CLI operations:

- callhome
- grep
- install
- ping
- ping6
- raid
- scp
- shell
- techsupport
- traceroute
- traceroute6

videooptimization

Videooptimization

The entities on which you can perform NetScaler CLI operations:

- videooptimization-detectionaction
- videooptimization-detectionpolicy
- videooptimization-detectionpolicylabel
- videooptimization-globaldetection
- videooptimization-globalpacing
- videooptimization-pacingaction
- videooptimization-pacingpolicy
- videooptimization-pacingpolicylabel
- videooptimization-parameter
- videooptimization-stats
- videooptimization

videooptimization-detectionaction

The following operations can be performed on "videooptimization-detectionaction":

rm| unset| set| rename| show| add|

rm videooptimization detectionaction

Removes the specified video optimization detection action.

Synopsis

rm videooptimization detectionaction <name>

Arguments

name Name of the video optimization detection action to remove.

Example

rm videooptimization detectionAction act_before

unset videooptimization detectionaction

Use this command to remove videooptimization detectionaction settings.Refer to the set videooptimization detectionaction command for meanings of the arguments.

Synopsis

unset videooptimization detectionaction <name> -comment

set videooptimization detectionaction

Modifies the specified parameters of a video optimization detection action.

Synopsis

set videooptimization detectionaction <name>

Arguments

name Name of the video optimization detection action to be modified.

type Type of video optimization detection action.

Possible values: clear_text_pd, clear_text_abr, encrypted_abr, trigger_enc_abr, trigger_body_detection

comment Comment. Any type of information about this video optimization detection action.

Example

set videooptimization detectionaction act_vo -comment \"My action\"

rename videooptimization detectionaction

Renames a videooptimization detection action.

Synopsis

rename videooptimization detectionaction <name>@ <newName>@

Arguments

name Existing name of the videooptimization detection action.

newName New name for the videooptimization detection action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

Example

rename videooptimization detectionAction oldname newname

show videooptimization detectionaction

Name of the video optimization detection action for which to display the current settings. If you do not set this parameter current settings are shown for all video optimization detection actions.

Synopsis

show videooptimization detectionaction

Arguments

name Name of the video optimization detection action.

Output

stateflag type Type of video optimization detection action.

hits The number of times the action has been taken.

referenceCount The number of references to the action.

undefHits The number of times the action resulted in UNDEF.

comment Comment. Any type of information about this video optimization detection action.

builtin Flag to determine whether video optimization detection action is built-in or not

feature The feature to be checked while applying this config

devno count

Example

show videooptimization detectionaction DETECT_CLEARTEXT_PD

add videooptimization detectionaction

Creates a video optimization detection action, which specifies detected media type. Note: The following Detection actions are pre-configured by default:DETECT_CLEARTEXT_PD,

DETECT_CLEARTEXT_ABR, DETECT_ENCRYPTED_ABR, TRIGGER_ENC_ABR_DETECTION, TRIGGER_CT_ABR_BODY_DETECTION, RESET, DROP

Synopsis

add videooptimization detectionaction <name> -type <type>

Arguments

name Name for the video optimization detection action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

type Type of video optimization action. Available settings function as follows:

- clear_text_pd - Cleartext PD type is detected.
- clear_text_abr - Cleartext ABR is detected.
- encrypted_abr - Encrypted ABR is detected.
- trigger_enc_abr - Possible encrypted ABR is detected.
- trigger_body_detection - Possible cleartext ABR is detected. Triggers body content detection.

Possible values: clear_text_pd, clear_text_abr, encrypted_abr, trigger_enc_abr, trigger_body_detection

comment Comment. Any type of information about this video optimization detection action.

videooptimization-detectionpolicy

The following operations can be performed on "videooptimization-detectionpolicy":

set| add| rename| rm| stat| unset| show|

set videooptimization detectionpolicy

Modifies the specified parameter of the videooptimization detection policy.

Synopsis

set videooptimization detectionpolicy <name>

Arguments

name Name for the videooptimization detection policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters.Can be modified, removed or renamed.

rule Expression that determines which request or response match the video optimization detection policy.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the videooptimization detection action to perform if the request matches this videooptimization detection policy. Built-in actions should be used. These are:

- DETECT_CLEARTEXT_PD - Cleartext PD is detected and increment related counters.
- DETECT_CLEARTEXT_ABR - Cleartext ABR is detected and increment related counters.
- DETECT_ENCRYPTED_ABR - Encrypted ABR is detected and increment related counters.
- TRIGGER_ENC_ABR_DETECTION - This is potentially encrypted ABR. Internal traffic heuristics algorithms will further process traffic to confirm detection.
- TRIGGER_CT_ABR_BODY_DETECTION - This is potentially cleartext ABR. Internal traffic heuristics algorithms will further process traffic to confirm detection.
- RESET - Reset the client connection by closing it.
- DROP - Drop the connection without sending a response.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

comment Any type of information about this videooptimization detection policy.

logAction Name of the messagelog action to use for requests that match this policy.

Example

set videooptimization detectionPolicy pol1 -rule "HTTP.REQ.URL.CONTAINS(\".flv\")" -action DETECT_CLEARTEXT_PD

add videooptimization detectionpolicy

Creates a videooptimization detection policy, which specifies requests that the Citrix ADC intercepts and tries to detect media type.

Synopsis

add videooptimization detectionpolicy <name> -rule <expression> -action <string>

Arguments

name Name for the videooptimization detection policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters.Can be modified, removed or renamed.

rule Expression that determines which request or response match the video optimization detection policy.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the videooptimization detection action to perform if the request matches this videooptimization detection policy. Built-in actions should be used. These are:

- DETECT_CLEARTEXT_PD - Cleartext PD is detected and increment related counters.
- DETECT_CLEARTEXT_ABR - Cleartext ABR is detected and increment related counters.
- DETECT_ENCRYPTED_ABR - Encrypted ABR is detected and increment related counters.
- TRIGGER_ENC_ABR_DETECTION - This is potentially encrypted ABR. Internal traffic heuristics algorithms will further process traffic to confirm detection.

- TRIGGER_CT_ABR_BODY_DETECTION - This is potentially cleartext ABR. Internal traffic heuristics algorithms will further process traffic to confirm detection.
- RESET - Reset the client connection by closing it.
- DROP - Drop the connection without sending a response.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

comment Any type of information about this videooptimization detection policy.

logAction Name of the messagelog action to use for requests that match this policy.

Example

i) add videooptimization detectionPolicy pol1 -rule "HTTP.REQ.URL.CONTAINS(\".mov\")" -action DETECT_CLEARTEXT_PD

rename videooptimization detectionpolicy

Renames the specified videooptimization detection policy.

Synopsis

rename videooptimization detectionpolicy <name>@ <newName>@

Arguments

name Existing name of the videooptimization detection policy.

newName New name for the videooptimization detection policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

Example

rename videooptimization detectionpolicy oldname newname

rm videooptimization detectionpolicy

Removes the specified videooptimization detection policy.

Synopsis

rm videooptimization detectionpolicy <name>

Arguments

name Name for the videooptimization detection policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters.Can be modified, removed or renamed.

Example

rm videooptimization detectionPolicy pol1

stat videooptimization detectionpolicy

Displays statistics for all video optimization detection policies currently configured on the Citrix ADC, or detailed statistics for the specified policy.

Synopsis

stat videooptimization detectionpolicy

Arguments

name Name of the Video Optimization detection policy for which to show detailed statistics.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Policy undef hits (Undefhits) Number of undef hits on the policy

Related Commands

- stat videooptimization pacingpolicylabel

unset videooptimization detectionpolicy

Removes the settings of an existing videooptimization detection policy. Attributes for which a default value is available revert to their default values. See the set videooptimization detection policy command for descriptions of the parameters..Refer to the set videooptimization detectionpolicy command for meanings of the arguments.

Synopsis

unset videooptimization detectionpolicy <name>

Example

unset videooptimization detectionPolicy pol1 -undefAction

show videooptimization detectionpolicy

Displays the current settings for the specified videooptimization detection policy.

Synopsis

show videooptimization detectionpolicy show videooptimization detectionpolicy stats - alias for 'stat videooptimization detectionpolicy'

Arguments

name Name of the videooptimization detection policy for which to display settings.Must provide policy name.

Output

stateflag rule Expression that determines which request or response match the video optimization detection policy.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.

- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the videooptimization detection action to perform if the request matches this videooptimization detection policy. Built-in actions should be used. These are:

- DETECT_CLEARTEXT_PD - Cleartext PD is detected and increment related counters.
- DETECT_CLEARTEXT_ABR - Cleartext ABR is detected and increment related counters.
- DETECT_ENCRYPTED_ABR - Encrypted ABR is detected and increment related counters.
- TRIGGER_ENC_ABR_DETECTION - This is potentially encrypted ABR. Internal traffic heuristics algorithms will further process traffic to confirm detection.
- TRIGGER_CT_ABR_BODY_DETECTION - This is potentially cleartext ABR. Internal traffic heuristics algorithms will further process traffic to confirm detection.
- RESET - Reset the client connection by closing it.
- DROP - Drop the connection without sending a response.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

hits Number of hits.

undefHits Number of policy UNDEF hits.

activePolicy Indicates whether policy is bound or not.

boundTo Location where policy is bound

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

comment Any type of information about this videooptimization detection policy.

logAction Name of the messagelog action to use for requests that match this policy.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

vserverType builtin Flag to determine if videooptimization detection policy is built-in or not

feature The feature to be checked while applying this config

type devno count

Example

show videooptimization detectionpolicy pol1

videooptimization-detectionpolicylabel

The following operations can be performed on "videooptimization-detectionpolicylabel":

rename| stat| rm| add| bind| unbind| show|

rename videooptimization detectionpolicylabel

Renames the specified videooptimization detection policy label.

Synopsis

rename videooptimization detectionpolicylabel <labelName>@ <newName>@

Arguments

labelName Current name of the videooptimization detection policy label.

newName New name for the videooptimization detection policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

Example

rename videooptimization detectionpolicylabel oldname newname

stat videooptimization detectionpolicylabel

Displays statistics for the specified videooptimization detection policy label. If no policy label name is provided, displays abbreviated statistics for all videooptimization detection policy labels currently configured on the Citrix ADC.

Synopsis

stat videooptimization detectionpolicylabel

Arguments

labelName Name of the videooptimization detection policy label.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy Label Hits (Hits) Number of times policy label was invoked.

Related Commands

- stat videooptimization pacingpolicylabel

rm videooptimization detectionpolicylabel

Removes a videooptimization detection policy label.

Synopsis

rm videooptimization detectionpolicylabel <labelName>

Arguments

labelName Name of the videooptimization detection policy label to remove.

Example

rm videooptimization detectionpolicylabel videoopt_label

add videooptimization detectionpolicylabel

Creates a user-defined videooptimization detection policy label, to which you can bind detection policies. A policy label is a tool for evaluating a set of policies in a specified order. By using a policy label, you can configure the videooptimization feature to choose the next policy, invoke a different policy label, or terminate policy evaluation completely by looking at whether the previous policy evaluated to TRUE or FALSE.

Synopsis

add videooptimization detectionpolicylabel <labelName>

Arguments

labelName Name for the Video optimization detection policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the videooptimization detection policy label is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my videooptimization detection policy label" or my videooptimization detection policy label').

policylabeltype Type of responses sent by the policies bound to this policy label. Types are:

- HTTP - HTTP responses.
- OTHERTCP - NON-HTTP TCP responses.

Possible values: videoopt_req, videoopt_res Default value: NS_PLTMAP_RSP_REQ

comment Any comments to preserve information about this videooptimization detection policy label.

Example

add videooptimization detectionpolicylabel videoopt_label

bind videooptimization detectionpolicylabel

Binds the specified videooptimization detection policy to the specified policy label.

Synopsis

bind videooptimization detectionpolicylabel <labelName> -policyName <string> -priority <positive_integer>

Arguments

labelName Name of the videooptimization detection policy label to which to bind the policy.

policyName Name of the policy to bind to the videooptimization detection policy label.

priority Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Must be unique within the label. Policies are evaluated in the order of their priority numbers , and the first policy that matches the request is applied. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is any thing other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.
- The expression evaluates to a priority number that is smaller than the current policys priority number.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured prior ity number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label and evaluate the specified policy label.

labelType Type of policy label to invoke. Available settings function as follows:

- vserver - Invoke an unnamed policy label associated with a virtual server.
- policylabel - Invoke a user-defined policy label.

Possible values: vserver, policylabel

labelName

- If labelType is policylabel, name of the policy label to invoke.
- If labelType is reqvserver or resvserver, name of the virtual server.

Example

i) bind videooptimization detectionpolicylabel videoopt_label -policyName pol_videoopt -priority 100
ii) bind videooptimization detectionpolicylabel videoopt_label -policyName pol_videoopt_2 -priority 200 -invoke vserver CURRENT

unbind videooptimization detectionpolicylabel

Unbinds the specified videooptimization detection policy from the specified policy label.

Synopsis

unbind videooptimization detectionpolicylabel <labelName> -policyName <string>

Arguments

labelName Name for the Video optimization detection policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the videooptimization detection policy label is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my videooptimization detection policy label" or my videooptimization detection policy label').

policyName The name of the policy to be unbound.

priority Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind videooptimization detectionpolicylabel videoopt_label pol_videoopt

show videooptimization detectionpolicylabel

Displays the current settings for the specified videooptimization detection policy label. If no policy label is specified, displays a list of all videooptimization detection policy labels currently configured on the Citrix ADC, with abbreviated settings.

Synopsis

show videooptimization detectionpolicylabel

Arguments

labelName Name of the videooptimization detection policy label.

Output

policylabeltype The type of the policy label.

stateflag numpol number of polices bound to label.

hits Number of times policy label was invoked.

policyName Name of the videooptimization policy.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label and evaluate the specified policy label.

labelType Type of policy label to invoke. Available settings function as follows:

- vserver - Invoke an unnamed policy label associated with a virtual server.
- policylabel - Invoke a user-defined policy label.

labelName

- If labelType is policylabel, name of the policy label to invoke.
- If labelType is reqvserver or resvserver, name of the virtual server.

flags comment Any comments to preserve information about this videooptimization detection policy label.

devno count

Example

i) show videooptimization detectionpolicylabel videoopt_label ii) show videooptimization detectionpolicylabel

videooptimization-globaldetection

The following operations can be performed on "videooptimization-globaldetection":

show| bind| unbind|

show videooptimization globaldetection

Displays the list of detection policies bound to the specified video optimization global detection bindpoint.If bindpoint is not specified, displays a list of all detection policies bound to video optimization global detection.

Synopsis

show videooptimization globaldetection

Arguments

type Specifies the bind point whose policies you want to display.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

Output

stateflag policyName Name of the videooptimization detection policy.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

numpol number of polices bound.

globalBindType devno count

Example

show videooptimization globaldetection

bind videooptimization globaldetection

Activates the specified videooptimization detectionpolicy for all requests and responses sent to the Citrix ADC.

Synopsis

bind videooptimization globaldetection -policyName <string> -priority <positive_integer>

Arguments

policyName Name of the video optimization policy to activate.

priority Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Policies are evaluated in the order of their priority numbers, and the first policy that matches the request is applied. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE.

type Bind point to which to bind the policy. Available settings function as follows:

- REQ_OVERRIDE - Request override. Binds the policy to the priority request queue.
- REQ_DEFAULT - Binds the policy to the default request queue.
- RES_OVERRIDE - Response override.
- RES_DEFAULT - Binds the policy to the default response queue.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

labelType Type of invocation, Available settings function as follows:

- vserver - Forward the request to the specified virtual server.
- policylabel - Invoke the specified policy label.

Possible values: vserver, policylabel

labelName Name of the policy label to invoke. If the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is policylabel.

Example

i)bind videooptimization globaldetection -policyName pol1 -priority 100

unbind videooptimization globaldetection

Unbind the specified videooptimization detectionpolicy from videooptimization globaldetection.

Synopsis

unbind videooptimization globaldetection -policyName <string>

Arguments

policyName Name of the policy to unbind.

type The bindpoint from which the policy is to be unbound.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

priority Priority of the videooptimization policy to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind videooptimization globaldetection pol1

videooptimization-globalpacing

The following operations can be performed on "videooptimization-globalpacing":

bind| unbind| show|

bind videooptimization globalpacing

Activates the specified videooptimization pacingpolicy for all requests and responses sent to the Citrix ADC. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

policyName Name of the video optimization pacing policy to activate.

priority Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Policies are evaluated in the order of their priority numbers, and the first policy that matches the request is applied. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE.

type Bind point to which to bind the policy. Available settings function as follows:

- REQ_OVERRIDE - Request override. Binds the policy to the priority request queue.
- REQ_DEFAULT - Binds the policy to the default request queue.
- RES_OVERRIDE - Response override.
- RES_DEFAULT - Binds the policy to the default response queue.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

labelType Type of invocation, Available settings function as follows:

- vserver - Forward the request to the specified virtual server.
- policylabel - Invoke the specified policy label.

Possible values: vserver, policylabel

labelName Name of the policy label to invoke. If the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is policylabel.

Example

i)bind videooptimization globalpacing -policyName pol1 -priority 100

unbind videooptimization globalpacing

Unbind the specified videooptimization pacingpolicy from videooptimization global pacing. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

policyName Name of the policy to unbind.

type The bindpoint from which the policy is to be unbound.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

priority Priority of the videooptimization policy to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind videooptimization globalpacing pol1

show videooptimization globalpacing

Displays the list of pacing policies bound to the specified video optimization global pacing bindpoint.If bindpoint is not specified, displays a list of all pacing policies bound to video optimization global pacing. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

type Specifies the bind point whose policies you want to display.

Possible values: REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

Output

stateflag policyName Name of the videooptimization pacing policy.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

numpol number of polices bound.

globalBindType devno count

Example

show videooptimization globalpacing

videooptimization-pacingaction

The following operations can be performed on "videooptimization-pacingaction":

add| set| rename| rm| unset| show|

add videooptimization pacingaction

Creates a video optimization pacing action, which applies the specified pacing rate. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

name Name for the video optimization pacing action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

rate ABR Video Optimization Pacing Rate (in Kbps) Default value: 1000 Minimum value: 1 Maximum value: 2147483647

comment Comment. Any type of information about this video optimization detection action.

set videooptimization pacingaction

Modifies the specified parameters of a video optimization pacing action. NOTE: This command is deprecated.

Synopsis

Arguments

name Name of the video optimization pacing action to be modified.

rate ABR Video Optimization Pacing Rate (in Kbps) Default value: 1000 Minimum value: 1 Maximum value: 2147483647

comment Comment. Any type of information about this video optimization detection action.

Example

set videooptimization pacingAction act_vo -comment \"My action\"

rename videooptimization pacingaction

Renames a videooptimization pacing action. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

name Existing name of the videooptimization pacing action.

newName New name for the videooptimization pacing action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

Example

rename videooptimization pacingAction oldname newname

rm videooptimization pacingaction

Removes the specified video optimization pacing action. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

name Name of the video optimization pacing action to remove.

Example

rm videooptimization pacingAction act_before

unset videooptimization pacingaction

Use this command to remove videooptimization pacingaction settings.Refer to the set videooptimization pacingaction command for meanings of the arguments.NOTE: This command is deprecated.

Synopsis

show videooptimization pacingaction

Name of the video optimization pacing action for which to display the current settings. If you do not set this parameter current settings are shown for all video optimization pacing actions. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

name Name of the video optimization pacing action.

Output

stateflag hits The number of times the action has been taken.

referenceCount The number of references to the action.

undefHits The number of times the action resulted in UNDEF.

rate ABR Video Optimization Pacing Rate (in Kbps)

comment Comment. Any type of information about this video optimization detection action.

builtin Flag to determine whether video optimization detection action is built-in or not

feature The feature to be checked while applying this config

devno count

Example

show videooptimization pacingaction myPacingAct1

videooptimization-pacingpolicy

The following operations can be performed on "videooptimization-pacingpolicy":

rename| add| set| stat| rm| show| unset|

rename videooptimization pacingpolicy

Renames the specified videooptimization pacing policy. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

name Existing name of the videooptimization pacing policy.

newName New name for the videooptimization pacing policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

Example

rename videooptimization pacingpolicy oldname newname

add videooptimization pacingpolicy

Creates a videooptimization pacing policy, which specifies requests that the Citrix ADC intercepts and applies specific pacing rate. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

name Name for the videooptimization pacing policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters.Can be modified, removed or renamed.

rule Expression that determines which request or response match the video optimization pacing policy.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the videooptimization pacing action to perform if the request matches this videooptimization pacing policy.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

comment Any type of information about this videooptimization pacing policy.

logAction Name of the messagelog action to use for requests that match this policy.

Example

i) add videooptimization pacingpolicy pol1 -rule "HTTP.REQ.URL.CONTAINS(\".mov\")" -action pacingAct1

set videooptimization pacingpolicy

Modifies the specified parameter of the videooptimization pacing policy. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

name Name for the videooptimization pacing policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters.Can be modified, removed or renamed.

rule Expression that determines which request or response match the video optimization pacing policy.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the videooptimization pacing action to perform if the request matches this videooptimization pacing policy.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

comment Any type of information about this videooptimization pacing policy.

logAction Name of the messagelog action to use for requests that match this policy.

Example

set videooptimization pacingPolicy pol1 -rule "HTTP.REQ.URL.CONTAINS(\".flv\")" -action pacingAct1

stat videooptimization pacingpolicy

Displays statistics for all video optimization pacing policies currently configured on the Citrix ADC, or detailed statistics for the specified policy. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

name Name of the Video Optimization Pacing policy for which to show detailed statistics.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Policy undef hits (Undefhits) Number of undef hits on the policy

Related Commands

- stat videooptimization pacingpolicylabel

rm videooptimization pacingpolicy

Removes the specified videooptimization pacing policy. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

name Name for the videooptimization pacing policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters.Can be modified, removed or renamed.

Example

rm videooptimization pacingPolicy pol1

show videooptimization pacingpolicy

Displays the current settings for the specified videooptimization pacing policy. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

name Name of the videooptimization pacing policy for which to display settings.Must provide policy name.

Output

stateflag rule Expression that determines which request or response match the video optimization pacing policy.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Name of the videooptimization pacing action to perform if the request matches this videooptimization pacing policy.

undefAction Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.

hits Number of hits.

undefHits Number of policy UNDEF hits.

activePolicy Indicates whether policy is bound or not.

boundTo Location where policy is bound

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

comment Any type of information about this videooptimization pacing policy.

logAction Name of the messagelog action to use for requests that match this policy.

labelType Type of policy label invocation.

labelName Name of the label to invoke if the current policy rule evaluates to TRUE.

vserverType builtin Flag to determine if videooptimization pacing policy is built-in or not

feature The feature to be checked while applying this config

devno count

Example

show videooptimization pacingpolicy pol1

unset videooptimization pacingpolicy

Removes the settings of an existing videooptimization pacing policy. Attributes for which a default value is available revert to their default values. See the set videooptimization detectionpolicy command for descriptions of the parameters..Refer to the set videooptimization pacingpolicy command for meanings of the arguments.NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Example

unset videooptimization pacingpolicy pol1 -undefAction

videooptimization-pacingpolicylabel

The following operations can be performed on "videooptimization-pacingpolicylabel":

add| rm| rename| bind| unbind| show| stat|

add videooptimization pacingpolicylabel

Creates a user-defined videooptimization pacing policy label, to which you can bind policies. A policy label is a tool for evaluating a set of policies in a specified order. By using a policy label, you can configure the videooptimization feature to choose the next policy, invoke a different policy label, or terminate policy evaluation completely by looking at whether the previous policy evaluated to TRUE or FALSE. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

labelName Name for the Video optimization pacing policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the videooptimization pacing policy label is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my videooptimization pacing policy label" or my videooptimization pacing policy label').

policylabeltype Type of responses sent by the policies bound to this policy label. Types are:

- HTTP - HTTP responses.
- OTHERTCP - NON-HTTP TCP responses.

Possible values: videoopt_req, videoopt_res Default value: NS_PLTMAP_RSP_REQ

comment Any comments to preserve information about this videooptimization pacing policy label.

Example

add videooptimization pacingpolicylabel videoopt_label

rm videooptimization pacingpolicylabel

Removes a videooptimization pacing policy label. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

labelName Name of the videooptimization pacing policy label to remove.

Example

rm videooptimization pacingpolicylabel videoopt_label

rename videooptimization pacingpolicylabel

Renames the specified videooptimization pacing policy label. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

labelName Current name of the videooptimization pacing policy label.

newName New name for the videooptimization pacing policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

Example

rename videooptimization pacingpolicylabel oldname newname

bind videooptimization pacingpolicylabel

Binds the specified videooptimization pacing policy to the specified policy label. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

labelName Name of the videooptimization pacing policy label to which to bind the policy.

policyName Name of the policy to bind to the videooptimization pacing policy label.

priority Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Must be unique within the label. Policies are evaluated in the order of their priority numbers , and the first policy that matches the request is applied. Minimum value: 1 Maximum value: 2147483647

gotoPriorityExpression Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is any thing other than END, the current policy label performs a NEXT.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.
- The expression evaluates to a priority number that is smaller than the current policys priority number.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured prior ity number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label and evaluate the specified policy label.

labelType Type of policy label to invoke. Available settings function as follows:

- vserver - Invoke an unnamed policy label associated with a virtual server.
- policylabel - Invoke a user-defined policy label.

Possible values: vserver, policylabel

labelName

- If labelType is policylabel, name of the policy label to invoke.
- If labelType is reqvserver or resvserver, name of the virtual server.

Example

i) bind videooptimization pacingpolicylabel videoopt_label -policyName pol_videoopt -priority 100 ii) bind videooptimization pacingpolicylabel videoopt_label -policyName pol_videoopt2 -priority 200 -invoke vserver CURRENT

unbind videooptimization pacingpolicylabel

Unbinds the specified videooptimization pacing policy from the specified policy label. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

labelName Name for the Video optimization pacing policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period

(.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the videooptimization pacing policy label is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my videooptimization pacing policy label" or my videooptimization pacing policy label').

policyName The name of the policy to be unbound.

priority Priority of the NOPOLICY to be unbound. Minimum value: 1 Maximum value: 2147483647

Example

unbind videooptimization pacingpolicylabel videoopt_label pol_videoopt

show videooptimization pacingpolicylabel

Displays the current settings for the specified videooptimization pacing policy label. If no policy label is specified, displays a list of all videooptimization pacing policy labels currently configured on the Citrix ADC, with abbreviated settings. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

labelName Name of the videooptimization pacing policy label.

Output

policylabeltype The type of the policy label.

stateflag numpol number of polices bound to label.

hits Number of times policy label was invoked.

policyName Name of the videooptimization policy.

priority Specifies the priority of the policy.

gotoPriorityExpression Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

invoke If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label and evaluate the specified policy label.

labelType Type of policy label to invoke. Available settings function as follows:

- vserver - Invoke an unnamed policy label associated with a virtual server.
- policylabel - Invoke a user-defined policy label.

labelName

- If labelType is policylabel, name of the policy label to invoke.
- If labelType is reqvserver or resvserver, name of the virtual server.

flags comment Any comments to preserve information about this videooptimization pacing policy label.

devno count

Example

i) show videooptimization pacingpolicylabel videoopt_label ii) show videooptimization pacingpolicylabel

stat videooptimization pacingpolicylabel

Displays statistics for the specified videooptimization pacing policy label. If no policy label name is provided, displays abbreviated statistics for all videooptimization pacing policy labels currently configured on the Citrix ADC. NOTE: This command is deprecated.As part of video optimization, the video pacing functionality is deprecated.

Synopsis

Arguments

labelName Name of the videooptimization pacing policy label.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy Label Hits (Hits) Number of times policy label was invoked.

Related Commands

- stat videooptimization detectionpolicylabel

videooptimization-parameter

The following operations can be performed on "videooptimization-parameter":

show| unset| set|

show videooptimization parameter

Displays the Video Optimization parameters.

Synopsis

show videooptimization parameter

Arguments

Output

RandomSamplingPercentage Used to configure a percentage of user sessions that will be randomly selected for not being optimized.

QUICPacingRate QUIC Video Pacing Rate (Kbbs)

Example

show videooptimization parameter

unset videooptimization parameter

Use this command to remove videooptimization parameter settings.Refer to the set videooptimization parameter command for meanings of the arguments.

Synopsis

unset videooptimization parameter -RandomSamplingPercentage

set videooptimization parameter

Modifies the specified Video Optimization parameters.

Synopsis

set videooptimization parameter

Arguments

RandomSamplingPercentage Random Sampling Percentage. Default value: 0 Minimum value: 0 Maximum value: 100

Example

set videooptimization parameter -randomSamplingPercentage 20.00

videooptimization-stats

The following operations can be performed on "videooptimization-stats":

show videooptimization stats

show videooptimization stats is an alias for stat videooptimization

Synopsis

show videooptimization stats - alias for 'stat videooptimization'

videooptimization

The following operations can be performed on "videooptimization":

stat videooptimization

Shows video optimization statistics

Synopsis

stat videooptimization

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

ClearText PD Video (CTPDVideo) Total number of progressive download HTTP videos

ClearText ABR Video (CTABVideo) Total number of adaptive bitrate HTTP videos

Encrypted ABR Video (EABVideo) Total number of adaptive bitrate HTTPS videos

QUIC Video (QUICVideo) Total number of QUIC videos

Other (videooptOther) Non video traffic

ClearText ABR Video Sessions (CTABVideoSes) Total number of adaptive bitrate HTTP video sessions

Encrypted ABR Video Sessions (EABVideoSes) Total number of adaptive bitrate HTTPS videos

QUIC Video Sessions (QUICVideoSes) Total number of sessions with QUIC videos

ClearText PD Bytes (CTPDVideoBytes) Total number of bytes for progressive download HTTP videos

ClearText ABR Bytes (CTABVideoBytes) Total number of bytes for adaptive bitrate HTTP videos

Encrypted ABR Bytes (EABVideoBytes) Total number of bytes for adaptive bitrate HTTPS videos

QUIC Bytes (QUICVideoBytes) Total number of bytes for QUIC videos

Other (videooptOtherBytes) Total number of bytes for non video traffic

Related Commands

- stat videooptimization pacingpolicylabel

vpn

vpn-alwaysONProfile

The following operations can be performed on "vpn-alwaysONProfile":

set| rm| unset| show| add|

set vpn alwaysONProfile

Modifies the specified parameters for AlwaysON profile.

Synopsis

set vpn alwaysONProfile <name>

Arguments

name Name for the AlwaysON profile

networkAccessOnVPNFailure Option to block network traffic when tunnel is not established(and the config requires that tunnel be established). When set to onlyToGateway, the network traffic to and from the client (except Gateway IP) is blocked. When set to fullAccess, the network traffic is not blocked

Possible values: onlyToGateway, fullAccess Default value: fullAccess,

clientControl Allow/Deny user to log off and connect to another Gateway

Possible values: ALLOW, DENY Default value: DENY

locationBasedVPN Option to decide if tunnel should be established when in enterprise network. When locationBasedVPN is remote, client tries to detect if it is located in enterprise network or not and establishes the tunnel if not in enterprise network. Dns suffixes configured using -add dns suffix- are used to decide if the client is in the enterprise network or not. If the resolution of the DNS suffix results in private IP, client is said to be in enterprise network. When set to EveryWhere, the client skips the check to detect if it is on the enterprise network and tries to establish the tunnel

Possible values: Remote, Everywhere Default value: Remote

rm vpn alwaysONProfile

Removes a previously created AlwaysON device profile.

Synopsis

rm vpn alwaysONProfile <name>

Arguments

name Name of AlwaysON profile to remove

unset vpn alwaysONProfile

Use this command to remove vpn alwaysONProfile settings.Refer to the set vpn alwaysONProfile command for meanings of the arguments.

Synopsis

unset vpn alwaysONProfile <name>

show vpn alwaysONProfile

Displays information on AlwaysON profile

Synopsis

show vpn alwaysONProfile

Arguments

name name of AlwaysON profile.

Output

networkAccessOnVPNFailure Option to block network traffic when tunnel is not established(and the config requires that tunnel be established). When set to onlyToGateway, the network traffic to and from the client (except Gateway IP) is blocked. When set to fullAccess, the network traffic is not blocked

clientControl Allow/Deny user to log off and connect to another Gateway

locationBasedVPN Option to decide if tunnel should be established when in enterprise network. When locationBasedVPN is remote, client tries to detect if it is located in enterprise network or not and establishes the tunnel if not in enterprise network. Dns suffixes configured using -add dns suffix- are used to decide if the client is in the enterprise network or not. If the resolution of the DNS

suffix results in private IP, client is said to be in enterprise network. When set to EveryWhere, the client skips the check to detect if it is on the enterprise network and tries to establish the tunnel

devno count stateflag

Example

show vpn alwaysONProfile AP1

add vpn alwaysONProfile

Creates an AlwaysON profile

Synopsis

add vpn alwaysONProfile <name>

Arguments

name name of AlwaysON profile

networkAccessOnVPNFailure Option to block network traffic when tunnel is not established(and the config requires that tunnel be established). When set to onlyToGateway, the network traffic to and from the client (except Gateway IP) is blocked. When set to fullAccess, the network traffic is not blocked

Possible values: onlyToGateway, fullAccess Default value: fullAccess,

clientControl Allow/Deny user to log off and connect to another Gateway

Possible values: ALLOW, DENY Default value: DENY

locationBasedVPN Option to decide if tunnel should be established when in enterprise network. When locationBasedVPN is remote, client tries to detect if it is located in enterprise network or not and establishes the tunnel if not in enterprise network. Dns suffixes configured using -add dns suffix- are used to decide if the client is in the enterprise network or not. If the resolution of the DNS suffix results in private IP, client is said to be in enterprise network. When set to EveryWhere, the client skips the check to detect if it is on the enterprise network and tries to establish the tunnel

Possible values: Remote, Everywhere Default value: Remote

vpn-clientlessAccessPolicy

The following operations can be performed on "vpn-clientlessAccessPolicy":

show| add| set| rm|

show vpn clientlessAccessPolicy

Displays a clientless access policy.

Synopsis

show vpn clientlessAccessPolicy

Arguments

name Name of the clientless access policy to display.

Output

rule The rule used by the clientless access policy. Rules are combinations of expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide

profileName The profile to invoked for the clientless access.

undefAction The UNDEF action.

hits The number of times the policy evaluated to true.

undefHits The number of times the policy evaluation resulted in undefined processing.

activePolicy Indicates whether policy is bound or not.

boundTo Location where policy is bound.

priority Specifies the priority of the policy.

description Description of the clientless access policy.

isDefault A value of true is returned if it is a default vpnclientlessrwpolicy.

stateflag builtin Flag to determine if vpn clientless rewrite policy is built-in or not

feature The feature to be checked while applying this config

devno count

add vpn clientlessAccessPolicy

Adds a clientless access policy, which enables users to log on using a web browser and connect to the bookmarked web address without requiring the user to install a software plug-in.

Synopsis

add vpn clientlessAccessPolicy <name> <rule> <profileName>

Arguments

name Name of the new clientless access policy.

rule Expression, or name of a named expression, specifying the traffic that matches the policy.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

profileName Name of the profile to invoke for the clientless access.

set vpn clientlessAccessPolicy

Adds a new rule to be used by an existing clientless access policy that includes a simple expression that specifies the conditions for which the policy is enforced.

Synopsis

set vpn clientlessAccessPolicy <name>

Arguments

name Name of the existing clientless access policy to modify.

rule Expression, or name of a named expression, specifying the traffic that matches the policy.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.

- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

profileName Name of the profile to invoke for the clientless access.

rm vpn clientlessAccessPolicy

Removes a clientless access policy.

Synopsis

rm vpn clientlessAccessPolicy <name>

Arguments

name Name of the clientless access policy to remove.

vpn-clientlessAccessProfile

The following operations can be performed on "vpn-clientlessAccessProfile":

set| add| unset| rm| show|

set vpn clientlessAccessProfile

Modifies the settings for an existing clientless access profile.

Synopsis

set vpn clientlessAccessProfile <profileName>

Arguments

profileName Name of the clientless access profile to modify.

URLRewritePolicyLabel Name of the configured URL rewrite policy label. If you do not specify a policy label name, then URLs are not rewritten.

JavaScriptRewritePolicyLabel Name of the configured JavaScript rewrite policy label. If you do not specify a policy label name, then JAVA scripts are not rewritten.

ReqHdrRewritePolicyLabel Name of the configured Request rewrite policy label. If you do not specify a policy label name, then requests are not rewritten.

ResHdrRewritePolicyLabel Name of the configured Response rewrite policy label.

RegexForFindingURLinJavaScript Name of the pattern set that contains the regular expressions, which match the URL in Java script.

RegexForFindingURLinCSS Name of the pattern set that contains the regular expressions, which match the URL in the CSS.

RegexForFindingURLinXComponent Name of the pattern set that contains the regular expressions, which match the URL in X Component.

RegexForFindingURLinXML Name of the pattern set that contains the regular expressions, which match the URL in XML.

RegexForFindingCustomURLs Name of the pattern set that contains the regular expressions, which match the URLs in the custom content type other than HTML, CSS, XML, XCOMP, and JavaScript. The custom content type should be included in the patset ns_cvpn_custom_content_types.

ClientConsumedCookies Specify the name of the pattern set containing the names of the cookies, which are allowed between the client and the server. If a pattern set is not specified, Citrix Gateway does not allow any cookies between the client and the server. A cookie that is not specified in the pattern set is handled by Citrix Gateway on behalf of the client.

requirePersistentCookie Specify whether a persistent session cookie is set and accepted for clientless access. If this parameter is set to ON, COM objects, such as MSOffice, which are invoked by the browser can access the files using clientless access. Use caution because the persistent cookie is stored on the disk.

Possible values: ON, OFF Default value: OFF

add vpn clientlessAccessProfile

Adds a collection of settings that allows clientless access to a given application. Settings include the policies to specify whether to rewrite a URL, rules to find the URLs within various web content-types, and a set of cookies that are required to be present on the client machine.

Synopsis

add vpn clientlessAccessProfile <profileName>

Arguments

profileName Name for the Citrix Gateway clientless access profile. Must begin with an ASCII alphabetic or underscore (_) character, and must consist only of ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the profile is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

unset vpn clientlessAccessProfile

Resets the attributes of the specified clientless access profile. Attributes for which a default value is available revert to their default values. Refer to the set vpn clientlessAccessProfile command for a description of the parameters..Refer to the set vpn clientlessAccessProfile command for meanings of the arguments.

Synopsis

unset vpn clientlessAccessProfile <profileName>

rm vpn clientlessAccessProfile

Removes a clientless access profile.

Synopsis

rm vpn clientlessAccessProfile <profileName>

Arguments

profileName Name of the clientless access profile to remove.

show vpn clientlessAccessProfile

Displays information about all the configured clientless access profiles, or displays detailed information about the specified clientless access profile.

Synopsis

show vpn clientlessAccessProfile

Arguments

profileName Name of the clientless access profile for which to display detailed information.

Output

stateflag URLRewritePolicyLabel Name of the configured URL rewrite policy label. If you do not specify a policy label name, then URLs are not rewritten.

JavaScriptRewritePolicyLabel Name of the configured JavaScript rewrite policy label. If you do not specify a policy label name, then JAVA scripts are not rewritten.

CSSRewritePolicyLabel The configured CSS rewrite policylabel.

XMLRewritePolicyLabel The configured XML rewrite policylabel.

XComponentRewritePolicyLabel The configured X-Component rewrite policylabel.

ReqHdrRewritePolicyLabel Name of the configured Request rewrite policy label. If you do not specify a policy label name, then requests are not rewritten.

ResHdrRewritePolicyLabel Name of the configured Response rewrite policy label.

RegexForFindingURLinJavaScript Name of the pattern set that contains the regular expressions, which match the URL in Java script.

RegexForFindingURLinCSS Name of the pattern set that contains the regular expressions, which match the URL in the CSS.

RegexForFindingURLinXComponent Name of the pattern set that contains the regular expressions, which match the URL in X Component.

RegexForFindingURLinXML Name of the pattern set that contains the regular expressions, which match the URL in XML.

RegexForFindingCustomURLs Name of the pattern set that contains the regular expressions, which match the URLs in the custom content type other than HTML, CSS, XML, XCOMP, and JavaScript. The custom content type should be included in the patset ns_cvpn_custom_content_types.

ClientConsumedCookies Specify the name of the pattern set containing the names of the cookies, which are allowed between the client and the server. If a pattern set is not specified, Citrix Gateway does not allow any cookies between the client and the server. A cookie that is not specified in the pattern set is handled by Citrix Gateway on behalf of the client.

requirePersistentCookie Specify whether a persistent session cookie is set and accepted for clientless access. If this parameter is set to ON, COM objects, such as MSOffice, which are

invoked by the browser can access the files using clientless access. Use caution because the persistent cookie is stored on the disk.

isDefault A value of true is returned if it is a default vpnclientlessrwprofile.

description Description of the clientless access profile.

builtin Flag to determine if vpn clientless rewrite profile is built-in or not

feature The feature to be checked while applying this config

devno count

Vpn

The entities on which you can perform NetScaler CLI operations:

- vpn-alwaysONProfile
- vpn-clientlessAccessPolicy
- vpn-clientlessAccessProfile
- vpn-epaprofile
- vpn-eula
- vpn-formSSOAction
- vpn-global
- vpn-icaConnection
- vpn-icaDtlsConnection
- vpn-intranetApplication
- vpn-nextHopServer
- vpn-parameter
- vpn-pcoipConnection
- vpn-pcoipProfile
- vpn-pcoipVserverProfile
- vpn-portaltheme
- vpn-samlSSOProfile
- vpn-sessionAction
- vpn-sessionPolicy

- vpn-sfconfig
- vpn-stats
- vpn-storeinfo
- vpn-trafficAction
- vpn-trafficPolicy
- vpn-url
- vpn-urlAction
- vpn-urlPolicy
- vpn
- vpn-vserver

vpn-epaprofile

The following operations can be performed on "vpn-epaprofile":

rm| show| add|

rm vpn epaprofile

Removes a previously created EPA device profile. NOTE: This command is deprecated.Depricated AdvanceEPA Option

Synopsis

Arguments

name Name of EPA device profile to remove

show vpn epaprofile

Displays information on device profile NOTE: This command is deprecated.Depricated AdvanceEPA Option

Synopsis

Arguments

name name of device profile.

Output

data The XML data associated with the device profile

devno count stateflag

Example

show vpn deviceprofile DP1

add vpn epaprofile

Creates an advanced pre-authentication EPA device profile with XML data NOTE: This command is deprecated.Depricated AdvanceEPA Option

Synopsis

Arguments

name name of device profile

fileName filename of the deviceprofile data xml

data deviceprofile data xml

vpn-eula

The following operations can be performed on "vpn-eula":

rm| add| show|

rm vpn eula

Removes a eula entity if exists

Synopsis

rm vpn eula <name>

Arguments

name Name of the eula to be removed

Example

rm vpn eula eulaname

add vpn eula

Add a new eula entity.

Synopsis

add vpn eula <name>

Arguments

name Name for the eula

Example

add vpn eula eulaname

show vpn eula

Displays information about all the configured eulas.

Synopsis

show vpn eula

Arguments

name Name for the eula

Output

devno count stateflag

vpn-formSSOAction

The following operations can be performed on "vpn-formSSOAction":

unset| show| rm| add| set|

unset vpn formSSOAction

Use this command to remove vpn formSSOAction settings.Refer to the set vpn formSSOAction command for meanings of the arguments.

Synopsis

unset vpn formSSOAction <name>

show vpn formSSOAction

Displays the attributes of a form-based single sign-on profile.

Synopsis

show vpn formSSOAction

Arguments

name Name of the form-based single sign-on profile.

Output

actionURL Root-relative URL to which the completed form is submitted.

userField Username field.

passwdField Password field.

responsesize Maximum number of bytes to allow in the response size. Specifies the number of bytes in the response to be parsed for extracting the forms.

nameValuePair Form attributes and their values to be submitted.

nvtype Bypass Form extraction

ssoSuccessRule Rule to be evaluated to check whether sso succeeded or not.

submitMethod Form Submit method.

devno count stateflag

rm vpn formSSOAction

Removes a configured form-based single sign-on profile.

Synopsis

rm vpn formSSOAction <name>

Arguments

name Name of the form-based single sign-on profile to remove.

add vpn formSSOAction

Creates a form-based single sign-on profile. Form based single sign-on allows users to log on one time to all protected applications in your network. Users can access web applications that require an HTML form-based logon without having to type their password again.

Synopsis

add vpn formSSOAction <name> -actionURL <URL> -userField <string> -passwdField <string> -ssoSuccessRule <expression>

Arguments

name Name for the form based single sign-on profile.

actionURL Root-relative URL to which the completed form is submitted.

userField Name of the form field in which the user types in the user ID.

passwdField Name of the form field in which the user types in the password.

ssoSuccessRule Expression that defines the criteria for SSO success. Expression such as checking for cookie in the response is a common example.

nameValuePair Other name-value pair attributes to send to the server, in addition to sending the user name and password. Value names are separated by an ampersand (&), such as in name1=value1&name2=value2.

responsesize Maximum number of bytes to allow in the response size. Specifies the number of bytes in the response to be parsed for extracting the forms. Default value: 8096 Minimum value: 0

nvtype How to process the name-value pair. Available settings function as follows:

- STATIC - The administrator-configured values are used.
- DYNAMIC - The response is parsed, the form is extracted, and then submitted.

Possible values: STATIC, DYNAMIC Default value: DYNAMIC

submitMethod HTTP method (GET or POST) used by the single sign-on form to send the logon credentials to the logon server.

Possible values: GET, POST Default value: GET

set vpn formSSOAction

Modifies the parameters of an existing form-based single sign-on profile (or action).

Synopsis

set vpn formSSOAction <name>

Arguments

name Name for the form based single sign-on profile.

actionURL Root-relative URL to which the completed form is submitted.

userField Name of the form field in which the user types in the user ID.

passwdField Name of the form field in which the user types in the password.

ssoSuccessRule Expression that defines the criteria for SSO success. Expression such as checking for cookie in the response is a common example.

responsesize Maximum number of bytes to allow in the response size. Specifies the number of bytes in the response to be parsed for extracting the forms. Default value: 8096 Minimum value: 0

nameValuePair Other name-value pair attributes to send to the server, in addition to sending the user name and password. Value names are separated by an ampersand (&), such as in name1=value1&name2=value2.

nvtype How to process the name-value pair. Available settings function as follows:

- STATIC - The administrator-configured values are used.
- DYNAMIC - The response is parsed, the form is extracted, and then submitted.

Possible values: STATIC, DYNAMIC Default value: DYNAMIC

submitMethod HTTP method (GET or POST) used by the single sign-on form to send the logon credentials to the logon server.

Possible values: GET, POST Default value: GET

vpn-global

The following operations can be performed on "vpn-global":

unbind| bind| show|

unbind vpn global

Unbinds Citrix Gateway policies to the virtual server globally.

Synopsis

unbind vpn global [-policyName <string>]

Arguments

policyName Name of the policy to unbind globally.

secondary Bind the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only to a primary authentication server but also to a secondary authentication server. User groups are aggregated across both authentication servers. The user name must be exactly the same on both authentication servers, but the authentication servers can require different passwords.

groupExtraction Bind the Authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called it primary and/or secondary authentication has succeeded.

intranetDomain A conflicting intranet domain name to be unbound.

intranetApplication The name of a VPN intranet application to be unbound.

nextHopServer The name of the next hop server to be unbound globally.

urlName The name of a VPN url to be unbound from vpn global.

intranetIP The intranet IP address or range to be unbound.

netmask The intranet IP or range's netmask to be unbound from vpn global.

intranetIP6 The intranet ip address or range to be unbound.

numaddr The intranet ip or range's netmask to be unbound from vpn global. Minimum value: 1

staServer Secure Ticketing Authority (STA) server to be removed, in the format 'http(s)://IP/FQDN/URLPATH'

appController App Controller server to be removed, in the format 'http(s)://IP/FQDN'

sharefile ShareFile server to be removed, in the format 'IP:PORT / FQDN:PORT'

portaltheme Name of the Portal theme to unbind from vpnglobal

eula Name of the EULA to unbind from vpnglobal

certkeyName SSL certkey to use in signing tokens.

userDataEncryptionKey Certificate to be used for encrypting user data like KB Question and Answers, Alternate Email Address, etc.

cacert Name of the CA certificate to unbind.

bind vpn global

Binds Citrix Gateway entities, including policies, globally.

Synopsis

bind vpn global [-policyName <string>] [-staServer <URL>] [-cacert <string>]

Arguments

policyName Name of the policy to bind globally.

priority Integer specifying the policy's priority. The lower the priority number, the higher the policy's priority. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value: 0 Maximum value: 2147483647

secondary Bind the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only to a primary authentication server but also to a secondary authentication server. User groups are aggregated across both authentication servers. The user name must be exactly the same on both authentication servers, but the authentication servers can require different passwords.

groupExtraction Bind the Authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called it primary and/or secondary authentication has succeeded.

intranetDomain Intranet domain name for single sign-on.

intranetApplication Name of the intranet application to bind globally.

nextHopServer Name of the next hop server to bind globally.

urlName Name of the URL of the virtual server to bind globally.

intranetIP Range of IP addresses in an address pool or individual IP addresses to bind globally.

netmask The intranet ip or range's netmask.

intranetIP6 Starting address in the range of IPv6 addresses in an address pool or individual IPv6 addresses to bind globally.

numaddr The intranet ipv6 address. Minimum value: 1

staServer Web address of the Secure Ticketing Authority (STA) server to be bound globally, in the following format: 'http(s)://FQDN/URLPATH'

staAddressType Type of the STA server address(ipv4/v6).

Possible values: IPV4, IPV6

appController App Controller server, in the format 'http(s)://IP/FQDN'

sharefile ShareFile server, in the format 'IP:PORT / FQDN:PORT'

gotoPriorityExpression Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

portaltheme Portaltheme name to bind globally

eula EULA name to bind globally

certkeyName SSL certkey to use in signing tokens.

userDataEncryptionKey Certificate to be used for encrypting user data like KB Question and Answers, Alternate Email Address, etc.

cacert Name of the CA certificate.

crlCheck Rule to use for the CRL corresponding to the CA certificate during client authentication. Available settings function as follows:

- MANDATORY - Deny SSL clients if the CRL is missing or expired, or the Next Update date is in the past, or the CRL is incomplete.
- OPTIONAL - Allow SSL clients if the CRL is missing or expired, or the Next Update date is in the past, or the CRL is incomplete, but deny if the client certificate is revoked in the CRL. If neither CRL nor OCSP option is specified while binding the CA certificate, this option is set to CRLCHECK OPTIONAL by default.

Possible values: Mandatory, Optional

ocspCheck Rule to use for the OCSP responder associated with the CA certificate during client authentication. If MANDATORY is specified, deny all SSL clients if the OCSP check fails because of connectivity issues with the remote OCSP server, or any other reason that prevents the OCSP check. With the OPTIONAL setting, allow SSL clients even if the OCSP check fails except when the client certificate is revoked.

Possible values: Mandatory, Optional

show vpn global

Shows the Citrix Gateway policies that are bound to the virtual server globally.

Synopsis

show vpn global

Arguments

Output

stateflag policyName The name of the policy.

priority Integer specifying the policy's priority. The lower the priority number, the higher the policy's priority. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000.

intranetDomain The conflicting intranet domain name.

intranetApplication The intranet vpn application.

nextHopServer The name of the next hop server bound to vpn global.

urlName The intranet url.

intranetIP The intranet ip address or range.

netmask The intranet ip address or range's netmask.

intranetIP6 The intranet ip address or range.

numaddr The intranet ip address or range's netmask.

staServer Configured Secure Ticketing Authority (STA) server.

staAddressType Type of the STA server address(ipv4/v6).

staAuthID Authority ID of the STA Server. Authority ID is used to match incoming STA Tickets in the SOCKS/CGP protocol with the right STA Server.

staState State of the STA Server. If Authority ID is set then STA Server is UP else DOWN.

appController Configured App Controller server.

sharefile Configured Sharefile server, in the format IP:PORT / FQDN:PORT

type Bindpoint to which the policy is bound

policySubType builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

secondary Bind the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only to a primary authentication server but also to a secondary authentication server. User groups are aggregated across both authentication servers. The user name must be exactly the same on both authentication servers, but the authentication servers can require different passwords.

groupExtraction Bind the Authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called it primary and/or secondary authentication has succeeded.

policyType Policy type (Classic/Advanced) to be bound.Used for display.

gotoPriorityExpression Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

globalBindType portaltheme Name of the portal theme bound to vpnglobal

eula Name of the EULA bound to vpnglobal

certkeyName SSL certkey to use in signing tokens.

cacert The name of the CA certificate binding.

crlCheck The state of the CRL check parameter (Mandatory/Optional).

ocspCheck The state of the OCSP check parameter (Mandatory/Optional).

userDataEncryptionKey Certificate to be used for encrypting user data like KB Question and Answers, Alternate Email Address, etc.

devno count

vpn-icaConnection

The following operations can be performed on "vpn-icaConnection":

show| kill|

show vpn icaConnection

Displays active connections that use the ICA proxy.

Synopsis

show vpn icaConnection

Arguments

userName User name for which to display connections.

TransProto Transport type for the existing Existing ICA conenction.

Possible values: TCP, UDP

Output

domain The domain name.

srcIP The client IP address.

srcPort The client port.

destIP The CPS server IP address.

destPort The CPS server port.

peId Core id of the session owner

stateflag devno count

kill vpn icaConnection

Terminates the specified ica connections.

Synopsis

kill vpn icaConnection

Arguments

userName User name for which ica connections needs to be terminated.

TransProto Transport Protocol for the Existing ICA conenction.

Possible values: TCP, UDP

all Terminate all active icaconnections.

Example

kill icaconnection -username joe

vpn-icaDtlsConnection

The following operations can be performed on "vpn-icaDtlsConnection":

show vpn icaDtlsConnection

Displays active connections that use the ICA proxy.

Synopsis

show vpn icaDtlsConnection

Arguments

userName User name for which to display connections.

Output

domain The domain name.

srcIP The client IP address.

srcPort The client port.

destIP The CPS server IP address.

destPort The CPS server port.

ChannelNumber The channel number.

peId Core id of the session owner

devno count stateflag

vpn-intranetApplication

The following operations can be performed on "vpn-intranetApplication":

rm| show| add|

rm vpn intranetApplication

Removes a configured intranet resource.

Synopsis

rm vpn intranetApplication <intranetApplication>

Arguments

intranetApplication Name of the intranet resource to remove.

show vpn intranetApplication

Displays information about all the configured intranet resources, or displays detailed information about the specified intranet resource.

Synopsis

show vpn intranetApplication

Arguments

intranetApplication Name of the intranet resource for which to display detailed information.

Output

protocol The IP protocol; for example, TCP, UDP or ANY

destIP The destination IP address.

netmask The destination netmask.

IPAddress The IP address for the application. This address is the real application server IP address.

hostName Name based interception. Names should be valid dns or wins names and will be resolved during interception on the sslvpn.

destPort The destination port.

clientApplication Names of the client applications, such as PuTTY and Xshell.

spoofIIP This specifies whether to spoof this application on the client.

interception The interception type; for example, proxy or transparent.

srcIP The source IP address.

srcPort The source port.

stateflag devno count

add vpn intranetApplication

Defines intranet applications to be made accessible through Citrix Gateway.

Synopsis

add vpn intranetApplication <intranetApplication> ((<destIP>) | <IPRange> | <hostName>) [-destPort <port>] [-interception (PROXY | TRANSPARENT)]

Arguments

intranetApplication Name of the intranet application.

protocol Protocol used by the intranet application. If protocol is set to BOTH, TCP and UDP traffic is allowed.

Possible values: TCP, UDP, ANY

destIP Destination IP address, IP range, or host name of the intranet application. This address is the server IP address.

netmask Destination subnet mask for the intranet application. Default value: 0xFFFFFFFF

IPRange If you have multiple servers in your network, such as web, email, and file shares, configure an intranet application that includes the IP range for all the network applications. This allows users to access all the intranet applications contained in the IP address range.

hostName Name of the host for which to configure interception. The names are resolved during interception when users log on with the Citrix Gateway Plug-in.

destPort Destination TCP or UDP port number for the intranet application. Use a hyphen to specify a range of port numbers, for example 90-95. Minimum value: 1

interception Interception mode for the intranet application or resource. Correct value depends on the type of client software used to make connections. If the interception mode is set to TRANSPARENT, users connect with the Citrix Gateway Plug-in for Windows. With the PROXY setting, users connect with the Citrix Gateway Plug-in for Java.

Possible values: PROXY, TRANSPARENT

srcIP Source IP address. Required if interception mode is set to PROXY. Default is the loopback address, 127.0.0.1.

srcPort Source port for the application for which the Citrix Gateway virtual server proxies the traffic. If users are connecting from a device that uses the Citrix Gateway Plug-in for Java, applications must be configured manually by using the source IP address and TCP port values specified in the intranet application profile. If a port value is not set, the destination port value is used. Minimum value: 1

vpn-nextHopServer

The following operations can be performed on "vpn-nextHopServer":

show| rm| add|

show vpn nextHopServer

Displays information about all the configured next Citrix Gateway hop servers, or detailed information about the specified Citrix Gateway next hop server.

Synopsis

show vpn nextHopServer

Arguments

name Name of the Citrix Gateway next hop server for which to display detailed information. Maximum value: 32

Output

nextHopIP Next hop IP address.

nextHopFQDN Next hop FQDN.

resAddressType Next hop FQDN Address Type.

nextHopPort Next hop port number.

secure Next hop over secure connection.

stateflag devno count

Example

show vpn nexthopserver dh1

rm vpn nextHopServer

Removes a configured next hop server.

Synopsis

rm vpn nextHopServer <name>

Arguments

name Name of the next hop server to remove. Maximum value: 32

Example

rm vpn nexthopserver dh1

add vpn nextHopServer

Enables a Citrix Gateway appliance in the first DMZ to communicate with one or more Citrix Gateway appliances in the second DMZ.

Synopsis

add vpn nextHopServer <name> (<nextHopIP> | (-nextHopFQDN <string>)) <nextHopPort>

Arguments

name Name for the Citrix Gateway appliance in the first DMZ. Maximum value: 32

nextHopIP IP address of the Citrix Gateway proxy in the second DMZ.

nextHopFQDN FQDN of the Citrix Gateway proxy in the second DMZ.

resAddressType Address Type (IPV4/IPv6) of DNS name of nextHopServer FQDN.

Possible values: IPV4, IPV6 Minimum value: 1

nextHopPort Port number of the Citrix Gateway proxy in the second DMZ. Minimum value: 1 Maximum value: 65535

secure Use of a secure port, such as 443, for the double-hop configuration.

Possible values: ON, OFF Default value: OFF

Example

add vpn nexthopserver dh1 10.1.1.1 80 -secure OFF

vpn-parameter

The following operations can be performed on "vpn-parameter":

show| unset| set|

show vpn parameter

Displays the configured Citrix Gateway parameters.

Synopsis

show vpn parameter

Arguments

Output

name The VPN name.

httpPort The HTTP Port.

winsIP The WINS server IP address used for WINS host resolution by the VPN.

dnsVserverName The configured DNS vserver used for DNS host resolution by the VPN.

splitDns The VPN client SplitDns state.

icaUserAccounting RADIUS policy to use for user accounting

sessTimeout The session timeout, in minutes.

clientSecurity The client security check applied to client sessions. This is in the form of an expression. Expressions are simple conditions, such as a test for equality, applied to operands,

such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

clientSecurityGroup The client security group that will be assigned on failure of the client security check. Users can in general be organized into Groups. In this case, the Client Security Group may have a more restrictive security policy.

clientSecurityMessage The client security message that will be displayed on failure of the client security check.

clientSecurityLog Specifies whether or not to display all failed Client Security scans to the end user

Smartgroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

splitTunnel Send, through the tunnel, traffic only for intranet applications that are defined in Citrix Gateway. Route all other traffic directly to the Internet. The OFF setting routes all traffic through Citrix Gateway. With the REVERSE setting, intranet applications define the network traffic that is not intercepted. All network traffic directed to internal IP addresses bypasses the VPN tunnel, while other traffic goes through Citrix Gateway. Reverse split tunneling can be used to log all non-local LAN traffic. For example, if users have a home network and are logged on through the Citrix Gateway Plug-in, network traffic destined to a printer or another device within the home network is not intercepted.

localLanAccess Set local LAN access. If split tunneling is OFF, and you set local LAN access to ON, the local client can route traffic to its local interface. When the local area network switch is specified, this combination of switches is useful. The client can allow local LAN access to devices that commonly have non-routable addresses, such as local printers or local file servers.

rfc1918 Only allow RFC1918 local addresses when local LAN access feature is enabled.

spoofIIP Controls the Spoofing of Intranet IP to the Windows Applications by Windows VPN client when the end-user is connected to SSL VPN in '-splittunnel OFF' mode.

killConnections Determines whether Windows VPN client should kill all pre-existing connections; (for example, the connections existing before the end user logged in to SSL VPN) and prevent new incoming connections on the Windows Client system when the end user is connected to SSL VPN in '-splittunnel OFF' mode.

transparentInterception Allow access to network resources by using a single IP address and subnet mask or a range of IP addresses. The OFF setting sets the mode to proxy, in which you configure destination and source IP addresses and port numbers. If you are using the Citrix Gateway Plug-in for Windows, set this parameter to ON, in which the mode is set to transparent. If you are using the Citrix Gateway Plug-in for Java, set this parameter to OFF.

windowsClientType The windows client type.

defaultAuthorizationAction The Authentication Action, such as allow or deny.

authorizationGroup The authorization group applied to the session.

clientIdleTimeout The client idle timeout, in minutes.

clientIdleTimeoutWarning The time after which the client gets a timeout warning, in minutes.

proxy Proxy configuration for the session.

allProtocolProxy Address set for all proxies.

httpProxy IP address of the proxy server to be used for HTTP access for all subsequent connections to the internal network.

ftpProxy IP address of the proxy server to be used for FTP access for all subsequent connections to the internal network.

socksProxy IP address of the proxy server to be used for SOCKS access for all subsequent connections to the internal network.

gopherProxy IP address of the proxy server to be used for GOPHER access for all subsequent connections to the internal network.

sslProxy IP address of the proxy server to be used for SSL access for all subsequent connections to the internal network.

proxyException The Proxy Exception string that is configured in the Browser for bypassing the previously configured proxies. Allowed only if proxy type is Browser.

proxyLocalBypass Bypass proxy server for local addresses option in Internet Explorer and Firefox proxy server settings.

clientCleanupPrompt Prompt for client-side cache clean-up when a client-initiated session closes.

forceCleanup Whether or not to force a cleanup on exit from the VPN session.

clientOptions List of configured buttons(and/or menu options in the docked client) in the Windows VPN client.

clientConfiguration List of configured tabs in the Windows VPN client.

SSO Enable or Disable Single Sign-On.

ssoCredential Specify whether to use the primary or secondary authentication credentials for single sign-on to the server.

windowsAutoLogon Enable or Disable Windows Auto Logon.

useMIP Enables or disables the use of a Mapped IP address for the session.

useIIP Define IP address pool options. Available settings function as follows:

- SPILLOVER - When an address pool is configured and the mapped IP is used as an intranet IP address, the mapped IP address is used when an intranet IP address cannot be assigned.
- NOSPILLOVER - When intranet IP addresses are enabled and the mapped IP address is not used, the Transfer Login page appears for users who have used all available intranet IP addresses.
- OFF - Address pool is not configured.

clientDebug Whether or not to add debugging information to the activity log on the client.

loginScript Path to the logon script that is run when a session is established. Separate multiple scripts by using comma. A "$" in the path signifies that the word following the "$" is an environment variable.

logoutScript Path to the logout script. Separate multiple scripts by using comma. A "$" in the path signifies that the word following the "$" is an environment variable.

homePage The home page URL, or 'none'. 'none' is case sensitive.

icaProxy Enable ICA proxy to configure secure Internet access to servers running Citrix XenApp or XenDesktop by using Citrix Receiver instead of the Citrix Gateway Plug-in.

wihome Web address of the Web Interface server, such as http://<ipAddress>/Citrix/XenApp, or Receiver for Web, which enumerates the virtualized resources, such as XenApp, XenDesktop, and cloud applications. This web address is used as the home page in ICA proxy mode. If Client Choices is ON, you must configure this setting. Because the user can choose between FullClient and ICAProxy, the user may see a different home page. An Internet web site may appear if the

user gets the FullClient option, or a Web Interface site if the user gets the ICAProxy option. If the setting is not configured, the XenApp option does not appear as a client choice.

wihomeAddressType Type of the wihome address(IPV4/V6)

citrixReceiverHome Web address for the Citrix Receiver home page. Configure Citrix Gateway so that when users log on to the appliance, the Citrix Gateway Plug-in opens a web browser that allows single sign-on to the Citrix Receiver home page.

wiPortalMode Layout on the Access Interface. The COMPACT value indicates the use of small icons.

ClientChoices Provide users with multiple logon options. With client choices, users have the option of logging on by using the Citrix Gateway Plug-in for Windows, Citrix Gateway Plug-in for Java, the Web Interface, or clientless access from one location. Depending on how Citrix Gateway is configured, users are presented with up to three icons for logon choices. The most common are the Citrix Gateway Plug-in for Windows, Web Interface, and clientless access.

epaClientType Choose between two types of End point Windows Client a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed b) Activex Control - ActiveX control run by Microsoft Internet Explorer.

iipDnsSuffix The DNS suffix for the intranet IP address.

forcedTimeout The time, in minutes after which a timeout is forced.

forcedTimeoutWarning The time, in minutes, after which a timeout warning is issued.

ntDomain Single sign-on domain to use for single sign-on to applications in the internal network. This setting can be overwritten by the domain that users specify at the time of logon or by the domain that the authentication server returns.

clientlessVpnMode Whether clientless VPN is available to the session.

clientlessModeUrlEncoding URL encoding to be used for clientless mode.

clientlessPersistentCookie State of persistent cookies in clientless access mode. Persistent cookies are required for accessing certain features of SharePoint, such as opening and editing Microsoft Word, Excel, and PowerPoint documents hosted on the SharePoint server. A persistent cookie remains on the user device and is sent with each HTTP request. Citrix Gateway encrypts the persistent cookie before sending it to the plug-in on the user device, and refreshes the cookie

periodically as long as the session exists. The cookie becomes stale if the session ends. Available settings function as follows:

- ALLOW - Enable persistent cookies. Users can open and edit Microsoft documents stored in SharePoint.
- DENY - Disable persistent cookies. Users cannot open and edit Microsoft documents stored in SharePoint.
- PROMPT - Prompt users to allow or deny persistent cookies during the session. Persistent cookies are not required for clientless access if users do not connect to SharePoint.

emailHome Web address for the web-based email, such as Outlook Web Access.

allowedLoginGroups Specify groups that have permission to log on to Citrix Gateway. Users who do not belong to this group or groups are denied access even if they have valid credentials.

encryptCsecExp Enable encryption of client security expressions.

appTokenTimeout The timeout value in seconds for tokens to access XenMobile applications

mdxTokenTimeout Validity of MDX Token in minutes. This token is used for mdx services to access backend and valid HEAD and GET request.

UITHEME Set VPN UI Theme to Green-Bubble, Caxton or Custom; default is Caxton.

SecureBrowse Allow users to connect through Citrix Gateway to network resources from iOS and Android mobile devices with Citrix Receiver. Users do not need to establish a full VPN tunnel to access resources in the secure network.

storefronturl Web address for StoreFront to be used in this session for enumeration of resources from XenApp or XenDesktop.

kcdAccount The KCD account details to be used in SSO

clientversions checkversion api

rdpClientProfileName Name of the RDP profile associated with the vserver.

tag WindowsPluginUpgrade Option to set plugin upgrade behaviour for Win

MacPluginUpgrade Option to set plugin upgrade behaviour for Mac

LinuxPluginUpgrade Option to set plugin upgrade behaviour for Linux

iconWithReceiver Option to decide whether to show plugin icon along with receiver icon

userDomains List of user domains specified as comma seperated value

icaSessionTimeout Enable or disable ica session timeout. If enabled and in case AAA session gets terminated, ICA connections associated with that will also get terminated

alwaysONProfileName Name of the AlwaysON profile. The builtin profile named none can be used to explicitly disable AlwaysON.

autoProxyUrl URL to auto proxy config file

AdvancedClientlessVpnMode Option to enable/disable Advanced ClientlessVpnMode. Additionaly, it can be set to STRICT to block Classic ClientlessVpnMode while in AdvancedClientlessMode.

pcoipProfileName Name of the PCOIP profile.

backendServerSni enables sni extension for backend server handshakes

backendCertValidation enables backend server certificate validation

vpnsessionpolicyBindtype Indicates current bind type (Classic/Advanced) for VPN session policy across all bind entities

vpnsessionpolicyCount Count of VPN session policies across all bind entities

fqdnSpoofedIP Spoofed IP address range that can be used by client for FQDN based split tunneling

netmask The netmask for the spoofed ip address

SameSite SameSite attribute value for Cookies generated in VPN context. This attribute value will be appended only for the cookies which are specified in the builtin patset ns_cookies_samesite

maxIIPPerUser Maximum number of Intranet IP that can be assigned to a user from AAA group, VPN vserver or VPN global pool. This setting is not applicable for AAA user level Intranet IP configuration

unset vpn parameter

Removes global parameters for Citrix Gateway..Refer to the set vpn parameter command for meanings of the arguments.

Synopsis

unset vpn parameter

set vpn parameter

Sets global parameters for Citrix Gateway.

Synopsis

set vpn parameter [-clientSecurity <expression>] [-wihome <URL>]

Arguments

httpPort Destination port numbers other than port 80, added as a comma-separated list. Traffic to these ports is processed as HTTP traffic, which allows functionality, such as HTTP authorization and single sign-on to a web application to work. Minimum value: 1

winsIP WINS server IP address to add to Citrix Gateway for name resolution.

dnsVserverName Name of the DNS virtual server for the user session.

splitDns Route the DNS requests to the local DNS server configured on the user device, or Citrix Gateway (remote), or both.

Possible values: LOCAL, REMOTE, BOTH

icaUserAccounting The name of the radiusPolicy to use for RADIUS user accounting info on the session.

sessTimeout Number of minutes after which the session times out. Default value: 30 Minimum value: 1 Maximum value: 65535

clientSecurity Specify the client security check for the user device to permit a Citrix Gateway session. The web address or IP address is not included in the expression for the client security check.

clientSecurityGroup The client security group that will be assigned on failure of the client security check. Users can in general be organized into Groups. In this case, the Client Security Group may have a more restrictive security policy.

clientSecurityMessage The client security message that will be displayed on failure of the client security check.

clientSecurityLog Specifies whether or not to display all failed Client Security scans to the end user

Possible values: ON, OFF Default value: OFF

Smartgroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

splitTunnel Send, through the tunnel, traffic only for intranet applications that are defined in Citrix Gateway. Route all other traffic directly to the Internet. The OFF setting routes all traffic through Citrix Gateway. With the REVERSE setting, intranet applications define the network traffic that is not intercepted. All network traffic directed to internal IP addresses bypasses the VPN tunnel, while other traffic goes through Citrix Gateway. Reverse split tunneling can be used to log all non-local LAN traffic. For example, if users have a home network and are logged on through the Citrix Gateway Plug-in, network traffic destined to a printer or another device within the home network is not intercepted.

Possible values: ON, OFF, REVERSE Default value: OFF

localLanAccess Set local LAN access. If split tunneling is OFF, and you set local LAN access to ON, the local client can route traffic to its local interface. When the local area network switch is specified, this combination of switches is useful. The client can allow local LAN access to devices that commonly have non-routable addresses, such as local printers or local file servers.

Possible values: ON, OFF, FORCED Default value: OFF

rfc1918 As defined in the local area network, allow only the following local area network addresses to bypass the VPN tunnel when the local LAN access feature is enabled:

- 10...*,
- 172.16..,
- 192.168..

Possible values: ON, OFF Default value: OFF

killConnections Specify whether the Citrix Gateway Plug-in should disconnect all preexisting connections, such as the connections existing before the user logged on to Citrix Gateway, and prevent new incoming connections on the Citrix Gateway Plug-in for Windows and MAC when the user is connected to Citrix Gateway and split tunneling is disabled.

Possible values: ON, OFF Default value: OFF

transparentInterception Allow access to network resources by using a single IP address and subnet mask or a range of IP addresses. The OFF setting sets the mode to proxy, in which you configure destination and source IP addresses and port numbers. If you are using the Citrix

Gateway Plug-in for Windows, set this parameter to ON, in which the mode is set to transparent. If you are using the Citrix Gateway Plug-in for Java, set this parameter to OFF.

Possible values: ON, OFF Default value: OFF

defaultAuthorizationAction Specify the network resources that users have access to when they log on to the internal network. The default setting for authorization is to deny access to all network resources. Citrix recommends using the default global setting and then creating authorization policies to define the network resources users can access. If you set the default authorization policy to DENY, you must explicitly authorize access to any network resource, which improves security.

Possible values: ALLOW, DENY Default value: DENY

authorizationGroup Comma-separated list of groups in which the user is placed when none of the groups that the user is a part of is configured on Citrix Gateway. The authorization policy can be bound to these groups to control access to the resources.

clientIdleTimeout Time, in minutes, after which to time out the user session if Citrix Gateway does not detect mouse or keyboard activity. Minimum value: 1 Maximum value: 9999

proxy Set options to apply proxy for accessing the internal resources. Available settings function as follows:

- BROWSER - Proxy settings are configured only in Internet Explorer and Firefox browsers.
- NS - Proxy settings are configured on the Citrix ADC.
- OFF - Proxy settings are not configured.

Possible values: BROWSER, NS, OFF

allProtocolProxy IP address of the proxy server to use for all protocols supported by Citrix Gateway.

httpProxy IP address of the proxy server to be used for HTTP access for all subsequent connections to the internal network.

ftpProxy IP address of the proxy server to be used for FTP access for all subsequent connections to the internal network.

socksProxy IP address of the proxy server to be used for SOCKS access for all subsequent connections to the internal network.

gopherProxy IP address of the proxy server to be used for GOPHER access for all subsequent connections to the internal network.

sslProxy IP address of the proxy server to be used for SSL access for all subsequent connections to the internal network.

proxyException Proxy exception string that will be configured in the browser for bypassing the previously configured proxies. Allowed only if proxy type is Browser.

proxyLocalBypass Bypass proxy server for local addresses option in Internet Explorer and Firefox proxy server settings.

Possible values: ENABLED, DISABLED Default value: DISABLED

clientCleanupPrompt Prompt for client-side cache clean-up when a client-initiated session closes.

Possible values: ON, OFF Default value: ON

forceCleanup Force cache clean-up when the user closes a session. You can specify all, none, or any combination of the client-side items.

clientConfiguration Allow users to change client Debug logging level in Configuration tab of the Citrix Gateway Plug-in for Windows.

SSO Set single sign-on (SSO) for the session. When the user accesses a server, the user's logon credentials are passed to the server for authentication. NOTE : This configuration does not honor the following authentication types for security reason. BASIC, DIGEST, and NTLM (without Negotiate NTLM2 Key or Negotiate Sign Flag). Use VPN TrafficAction to configure SSO for these authentication types.

Possible values: ON, OFF Default value: OFF

ssoCredential Specify whether to use the primary or secondary authentication credentials for single sign-on to the server.

Possible values: PRIMARY, SECONDARY Default value: PRIMARY

windowsAutoLogon Enable or disable the Windows Auto Logon for the session. If a VPN session is established after this setting is enabled, the user is automatically logged on by using Windows credentials after the system is restarted.

Possible values: ON, OFF Default value: OFF

useMIP Enable or disable the use of a unique IP address alias, or a mapped IP address, as the client IP address for each client session. Allow Citrix Gateway to use the mapped IP address as an intranet IP address when all other IP addresses are not available. When IP pooling is configured and the mapped IP is used as an intranet IP address, the mapped IP address is used when an intranet IP address cannot be assigned.

Possible values: NS, OFF Default value: NS

useIIP Define IP address pool options. Available settings function as follows:

- SPILLOVER - When an address pool is configured and the mapped IP is used as an intranet IP address, the mapped IP address is used when an intranet IP address cannot be assigned.
- NOSPILLOVER - When intranet IP addresses are enabled and the mapped IP address is not used, the Transfer Login page appears for users who have used all available intranet IP addresses.
- OFF - Address pool is not configured.

Possible values: NOSPILLOVER, SPILLOVER, OFF Default value: NOSPILLOVER

loginScript Path to the logon script that is run when a session is established. Separate multiple scripts by using comma. A "$" in the path signifies that the word following the "$" is an environment variable.

logoutScript Path to the logout script. Separate multiple scripts by using comma. A "$" in the path signifies that the word following the "$" is an environment variable.

homePage Web address of the home page that appears when users log on. Otherwise, users receive the default home page for Citrix Gateway, which is the Access Interface.

icaProxy Enable ICA proxy to configure secure Internet access to servers running Citrix XenApp or XenDesktop by using Citrix Receiver instead of the Citrix Gateway Plug-in.

Possible values: ON, OFF Default value: OFF

wihome Web address of the Web Interface server, such as http://<ipAddress>/Citrix/XenApp, or Receiver for Web, which enumerates the virtualized resources, such as XenApp, XenDesktop, and cloud applications. This web address is used as the home page in ICA proxy mode. If Client Choices is ON, you must configure this setting. Because the user can choose between FullClient and ICAProxy, the user may see a different home page. An Internet web site may appear if the user gets the FullClient option, or a Web Interface site if the user gets the ICAProxy option. If the setting is not configured, the XenApp option does not appear as a client choice.

wihomeAddressType Type of the wihome address(IPV4/V6)

Possible values: IPV4, IPV6

citrixReceiverHome Web address for the Citrix Receiver home page. Configure Citrix Gateway so that when users log on to the appliance, the Citrix Gateway Plug-in opens a web browser that allows single sign-on to the Citrix Receiver home page.

wiPortalMode Layout on the Access Interface. The COMPACT value indicates the use of small icons.

Possible values: NORMAL, COMPACT

ClientChoices Provide users with multiple logon options. With client choices, users have the option of logging on by using the Citrix Gateway Plug-in for Windows, Citrix Gateway Plug-in for Java, the Web Interface, or clientless access from one location. Depending on how Citrix Gateway is configured, users are presented with up to three icons for logon choices. The most common are the Citrix Gateway Plug-in for Windows, Web Interface, and clientless access.

Possible values: ON, OFF Default value: OFF

iipDnsSuffix An intranet IP DNS suffix. When a user logs on to Citrix Gateway and is assigned an IP address, a DNS record for the user name and IP address combination is added to the Citrix Gateway DNS cache. You can configure a DNS suffix to append to the user name when the DNS record is added to the cache. You can reach to the host from where the user is logged on by using the user's name, which can be easier to remember than an IP address. When the user logs off from Citrix Gateway, the record is removed from the DNS cache.

forcedTimeout Force a disconnection from the Citrix Gateway Plug-in with Citrix Gateway after a specified number of minutes. If the session closes, the user must log on again. Minimum value: 1 Maximum value: 65535

forcedTimeoutWarning Number of minutes to warn a user before the user session is disconnected. Minimum value: 1 Maximum value: 255

ntDomain Single sign-on domain to use for single sign-on to applications in the internal network. This setting can be overwritten by the domain that users specify at the time of logon or by the domain that the authentication server returns.

clientlessVpnMode Enable clientless access for web, XenApp or XenDesktop, and FileShare resources without installing the Citrix Gateway Plug-in. Available settings function as follows:

- ON - Allow only clientless access.
- OFF - Allow clientless access after users log on with the Citrix Gateway Plug-in.
- DISABLED - Do not allow clientless access.

Possible values: ON, OFF, DISABLED Default value: OFF

clientlessModeUrlEncoding When clientless access is enabled, you can choose to encode the addresses of internal web applications or to leave the address as clear text. Available settings function as follows:

- OPAQUE - Use standard encoding mechanisms to make the domain and protocol part of the resource unclear to users.
- TRANSPARENT - Do not encode the web address and make it visible to users.
- ENCRYPT - Allow the domain and protocol to be encrypted using a session key. When the web address is encrypted, the URL is different for each user session for the same web resource. If users bookmark the encoded web address, save it in the web browser and then log off, they cannot connect to the web address when they log on and use the bookmark. If users save the encrypted bookmark in the Access Interface during their session, the bookmark works each time the user logs on.

Possible values: TRANSPARENT, OPAQUE, ENCRYPT Default value: OPAQUE

clientlessPersistentCookie State of persistent cookies in clientless access mode. Persistent cookies are required for accessing certain features of SharePoint, such as opening and editing Microsoft Word, Excel, and PowerPoint documents hosted on the SharePoint server. A persistent cookie remains on the user device and is sent with each HTTP request. Citrix Gateway encrypts the persistent cookie before sending it to the plug-in on the user device, and refreshes the cookie periodically as long as the session exists. The cookie becomes stale if the session ends. Available settings function as follows:

- ALLOW - Enable persistent cookies. Users can open and edit Microsoft documents stored in SharePoint.
- DENY - Disable persistent cookies. Users cannot open and edit Microsoft documents stored in SharePoint.
- PROMPT - Prompt users to allow or deny persistent cookies during the session. Persistent cookies are not required for clientless access if users do not connect to SharePoint.

Possible values: ALLOW, DENY, PROMPT Default value: DENY

emailHome Web address for the web-based email, such as Outlook Web Access.

allowedLoginGroups Specify groups that have permission to log on to Citrix Gateway. Users who do not belong to this group or groups are denied access even if they have valid credentials.

encryptCsecExp Enable encryption of client security expressions.

Possible values: ENABLED, DISABLED Default value: ENABLED

appTokenTimeout The timeout value in seconds for tokens to access XenMobile applications Default value: 100 Minimum value: 1 Maximum value: 255

mdxTokenTimeout Validity of MDX Token in minutes. This token is used for mdx services to access backend and valid HEAD and GET request. Default value: 10 Minimum value: 1 Maximum value: 1440

UITHEME Set VPN UI Theme to Green-Bubble, Caxton or Custom; default is Caxton.

Possible values: DEFAULT, GREENBUBBLE, CUSTOM

SecureBrowse Allow users to connect through Citrix Gateway to network resources from iOS and Android mobile devices with Citrix Receiver. Users do not need to establish a full VPN tunnel to access resources in the secure network.

Possible values: ENABLED, DISABLED Default value: ENABLED

storefronturl Web address for StoreFront to be used in this session for enumeration of resources from XenApp or XenDesktop.

kcdAccount The KCD account details to be used in SSO

clientversions checkversion api

rdpClientProfileName Name of the RDP profile associated with the vserver.

WindowsPluginUpgrade Option to set plugin upgrade behaviour for Win

Possible values: Always, Essential, Never Default value: Always

MacPluginUpgrade Option to set plugin upgrade behaviour for Mac

Possible values: Always, Essential, Never Default value: Always

LinuxPluginUpgrade Option to set plugin upgrade behaviour for Linux

Possible values: Always, Essential, Never Default value: Always

iconWithReceiver Option to decide whether to show plugin icon along with receiver icon

Possible values: ON, OFF Default value: OFF

icaSessionTimeout Enable or disable ica session timeout. If enabled and in case AAA session gets terminated, ICA connections associated with that will also get terminated

Possible values: ON, OFF Default value: OFF

alwaysONProfileName Name of the AlwaysON profile. The builtin profile named none can be used to explicitly disable AlwaysON.

autoProxyUrl URL to auto proxy config file

AdvancedClientlessVpnMode Option to enable/disable Advanced ClientlessVpnMode. Additionaly, it can be set to STRICT to block Classic ClientlessVpnMode while in AdvancedClientlessMode.

Possible values: ENABLED, DISABLED, STRICT Default value: DISABLED

pcoipProfileName Name of the PCOIP profile.

backendServerSni enables sni extension for backend server handshakes

Possible values: ENABLED, DISABLED Default value: DISABLED

backendCertValidation enables backend server certificate validation

Possible values: ENABLED, DISABLED Default value: DISABLED

fqdnSpoofedIP Spoofed IP address range that can be used by client for FQDN based split tunneling

netmask The netmask for the spoofed ip address

SameSite SameSite attribute value for Cookies generated in VPN context. This attribute value will be appended only for the cookies which are specified in the builtin patset ns_cookies_samesite

Possible values: None, LAX, STRICT

Example

set vpn parameter -httpport 80 90 -winsIP 192.168.0.220 -dnsVserverName mydns -sessTimeout 240

vpn-pcoipConnection

The following operations can be performed on "vpn-pcoipConnection":

show| kill|

show vpn pcoipConnection

Displays active PCOIP connections.

Synopsis

show vpn pcoipConnection

Arguments

userName User name for the PCOIP connections.

Output

srcIP The client IP address.

srcPort The client port.

destIP The VDA IP address.

destPort The VDA server port.

peId Core id of the session owner

stateflag devno count

kill vpn pcoipConnection

Terminates the specified connections.

Synopsis

kill vpn pcoipConnection

Arguments

userName User name for the PCOIP connections.

all All active pcoip connections.

Example

kill pcoipconnection -username joe

vpn-pcoipProfile

The following operations can be performed on "vpn-pcoipProfile":

unset| show| set| rm| add|

unset vpn pcoipProfile

Use this command to remove vpn pcoipProfile settings.Refer to the set vpn pcoipProfile command for meanings of the arguments.

Synopsis

unset vpn pcoipProfile <name>

show vpn pcoipProfile

Displays information on PCoIP profile

Synopsis

show vpn pcoipProfile

Arguments

name name of PCoIP profile.

Output

conServerUrl Connection server URL

icvVerification ICV verification for PCOIP transport packets.

sessionIdleTimeout PCOIP Idle Session timeout

devno count stateflag

Example

show vpn pcoipprofile Prof1

set vpn pcoipProfile

Modifies the specified parameters for PCoIP profile.

Synopsis

set vpn pcoipProfile <name>

Arguments

name Name for the PCoIP profile

conServerUrl Connection server URL

icvVerification ICV verification for PCOIP transport packets.

Possible values: ENABLED, DISABLED Default value: DISABLED

sessionIdleTimeout PCOIP Idle Session timeout Default value: 180 Minimum value: 30 Maximum value: 240

rm vpn pcoipProfile

Removes a previously created PCoIP profile.

Synopsis

rm vpn pcoipProfile <name>

Arguments

name Name of PCoIP profile to remove

add vpn pcoipProfile

Creates an PCoIP profile

Synopsis

add vpn pcoipProfile <name> -conServerUrl <URL>

Arguments

name name of PCoIP profile

conServerUrl Connection server URL

icvVerification ICV verification for PCOIP transport packets.

Possible values: ENABLED, DISABLED Default value: DISABLED

sessionIdleTimeout PCOIP Idle Session timeout Default value: 180 Minimum value: 30 Maximum value: 240

vpn-pcoipVserverProfile

The following operations can be performed on "vpn-pcoipVserverProfile":

rm| set| show| add| unset|

rm vpn pcoipVserverProfile

Removes a previously created PCoIP vserver profile.

Synopsis

rm vpn pcoipVserverProfile <name>

Arguments

name Name of PCoIP vserver profile to remove

set vpn pcoipVserverProfile

Modifies the specified parameters for PCoIP vserver profile.

Synopsis

set vpn pcoipVserverProfile <name>

Arguments

name Name for the PCoIP session profile

udpPort UDP port for PCoIP data traffic Default value: 4172

loginDomain Login domain for PCoIP users

show vpn pcoipVserverProfile

Displays information on PCoIP vserver profile

Synopsis

show vpn pcoipVserverProfile

Arguments

name name of PCoIP vserver profile.

Output

udpPort UDP port for PCoIP data traffic

loginDomain Login domain for PCoIP users

devno count stateflag

Example

show vpn pcoipserverprofile Prof1

add vpn pcoipVserverProfile

Creates an PCoIP vserver profile

Synopsis

add vpn pcoipVserverProfile <name> -loginDomain <string>

Arguments

name name of PCoIP vserver profile

loginDomain Login domain for PCoIP users

udpPort UDP port for PCoIP data traffic Default value: 4172

unset vpn pcoipVserverProfile

Use this command to remove vpn pcoipVserverProfile settings.Refer to the set vpn pcoipVserverProfile command for meanings of the arguments.

Synopsis

unset vpn pcoipVserverProfile <name> -udpPort

vpn-portaltheme

The following operations can be performed on "vpn-portaltheme":

rm| show| add|

rm vpn portaltheme

Removes a portaltheme entity

Synopsis

rm vpn portaltheme <name>

Arguments

name Name of the portal theme to remove.

Example

rm vpn portaltheme theme1

show vpn portaltheme

Displays information about all the configured portalthemes.

Synopsis

show vpn portaltheme

Arguments

name Name of portal theme to be displayed

Output

basetheme builtin Flag to determine if portaltheme is built-in or not

feature The feature to be checked while applying this config

devno count stateflag

add vpn portaltheme

Add a new portaltheme entity. The base theme should be either Default,Greenbubble,X1 or RfWebUI

Synopsis

add vpn portaltheme <name> -basetheme <basetheme>

Arguments

name Name of the uitheme

basetheme

Example

add vpn portaltheme theme1 -basetheme Default

vpn-samlSSOProfile

The following operations can be performed on "vpn-samlSSOProfile":

show| rm| add| unset| set|

show vpn samlSSOProfile

Displays information about all configured saml single sign-on profiles, or displays detailed information about the specified action.

Synopsis

show vpn samlSSOProfile

Arguments

name Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

Output

samlSigningCertName Name of the signing authority as given in the SAML server's SSL certificate.

assertionConsumerServiceURL URL to which the assertion is to be sent.

sendPassword Option to send password in assertion.

samlIssuerName The name to be used in requests sent from Citrix ADC to IdP to uniquely identify Citrix ADC.

relaystateRule Expression to extract relaystate to be sent along with assertion. Evaluation of this expression should return TEXT content. This is typically a target url to which user is redirected after the recipient validates SAML token

signatureAlg Algorithm to be used to sign/verify SAML transactions

digestMethod Algorithm to be used to compute/verify digest for SAML transactions

audience Audience for which assertion sent by IdP is applicable. This is typically entity name or url that represents ServiceProvider

NameIDFormat Format of Name Identifier sent in Assertion.

NameIDExpr Expression that will be evaluated to obtain NameIdentifier to be sent in assertion

Attribute1 Name of attribute1 that needs to be sent in SAML Assertion

Attribute2 Name of attribute2 that needs to be sent in SAML Assertion

Attribute3 Name of attribute3 that needs to be sent in SAML Assertion

Attribute4 Name of attribute4 that needs to be sent in SAML Assertion

Attribute5 Name of attribute5 that needs to be sent in SAML Assertion

Attribute6 Name of attribute6 that needs to be sent in SAML Assertion

Attribute7 Name of attribute7 that needs to be sent in SAML Assertion

Attribute8 Name of attribute8 that needs to be sent in SAML Assertion

Attribute9 Name of attribute9 that needs to be sent in SAML Assertion

Attribute10 Name of attribute10 that needs to be sent in SAML Assertion

Attribute11 Name of attribute11 that needs to be sent in SAML Assertion

Attribute12 Name of attribute12 that needs to be sent in SAML Assertion

Attribute13 Name of attribute13 that needs to be sent in SAML Assertion

Attribute14 Name of attribute14 that needs to be sent in SAML Assertion

Attribute15 Name of attribute15 that needs to be sent in SAML Assertion

Attribute16 Name of attribute16 that needs to be sent in SAML Assertion

Attribute1FriendlyName User-Friendly Name of attribute1 that needs to be sent in SAML Assertion

Attribute2FriendlyName User-Friendly Name of attribute2 that needs to be sent in SAML Assertion

Attribute3FriendlyName User-Friendly Name of attribute3 that needs to be sent in SAML Assertion

Attribute4FriendlyName User-Friendly Name of attribute4 that needs to be sent in SAML Assertion

Attribute5FriendlyName User-Friendly Name of attribute5 that needs to be sent in SAML Assertion

Attribute6FriendlyName User-Friendly Name of attribute6 that needs to be sent in SAML Assertion

Attribute7FriendlyName User-Friendly Name of attribute7 that needs to be sent in SAML Assertion

Attribute8FriendlyName User-Friendly Name of attribute8 that needs to be sent in SAML Assertion

Attribute9FriendlyName User-Friendly Name of attribute9 that needs to be sent in SAML Assertion

Attribute10FriendlyName User-Friendly Name of attribute10 that needs to be sent in SAML Assertion

Attribute11FriendlyName User-Friendly Name of attribute11 that needs to be sent in SAML Assertion

Attribute12FriendlyName User-Friendly Name of attribute12 that needs to be sent in SAML Assertion

Attribute13FriendlyName User-Friendly Name of attribute13 that needs to be sent in SAML Assertion

Attribute14FriendlyName User-Friendly Name of attribute14 that needs to be sent in SAML Assertion

Attribute15FriendlyName User-Friendly Name of attribute15 that needs to be sent in SAML Assertion

Attribute16FriendlyName User-Friendly Name of attribute16 that needs to be sent in SAML Assertion

Attribute1Format Format of Attribute1 to be sent in Assertion.

Attribute2Format Format of Attribute2 to be sent in Assertion.

Attribute3Format Format of Attribute3 to be sent in Assertion.

Attribute4Format Format of Attribute4 to be sent in Assertion.

Attribute5Format Format of Attribute5 to be sent in Assertion.

Attribute6Format Format of Attribute6 to be sent in Assertion.

Attribute7Format Format of Attribute7 to be sent in Assertion.

Attribute8Format Format of Attribute8 to be sent in Assertion.

Attribute9Format Format of Attribute9 to be sent in Assertion.

Attribute10Format Format of Attribute10 to be sent in Assertion.

Attribute11Format Format of Attribute11 to be sent in Assertion.

Attribute12Format Format of Attribute12 to be sent in Assertion.

Attribute13Format Format of Attribute13 to be sent in Assertion.

Attribute14Format Format of Attribute14 to be sent in Assertion.

Attribute15Format Format of Attribute15 to be sent in Assertion.

Attribute16Format Format of Attribute16 to be sent in Assertion.

Attribute1Expr Expression that will be evaluated to obtain attribute1's value to be sent in Assertion

Attribute2Expr Expression that will be evaluated to obtain attribute2's value to be sent in Assertion

Attribute3Expr Expression that will be evaluated to obtain attribute3's value to be sent in Assertion

Attribute4Expr Expression that will be evaluated to obtain attribute4's value to be sent in Assertion

Attribute5Expr Expression that will be evaluated to obtain attribute5's value to be sent in Assertion

Attribute6Expr Expression that will be evaluated to obtain attribute6's value to be sent in Assertion

Attribute7Expr Expression that will be evaluated to obtain attribute7's value to be sent in Assertion

Attribute8Expr Expression that will be evaluated to obtain attribute8's value to be sent in Assertion

Attribute9Expr Expression that will be evaluated to obtain attribute9's value to be sent in Assertion

Attribute10Expr Expression that will be evaluated to obtain attribute10's value to be sent in Assertion

Attribute11Expr Expression that will be evaluated to obtain attribute11's value to be sent in Assertion

Attribute12Expr Expression that will be evaluated to obtain attribute12's value to be sent in Assertion

Attribute13Expr Expression that will be evaluated to obtain attribute13's value to be sent in Assertion

Attribute14Expr Expression that will be evaluated to obtain attribute14's value to be sent in Assertion

Attribute15Expr Expression that will be evaluated to obtain attribute15's value to be sent in Assertion

Attribute16Expr Expression that will be evaluated to obtain attribute16's value to be sent in Assertion

encryptAssertion Option to encrypt assertion when Citrix ADC sends one.

samlSPCertName Name of the SSL certificate of peer/receving party using which Assertion is encrypted.

encryptionAlgorithm Algorithm to be used to encrypt SAML assertion

skewTime This option specifies the number of minutes on either side of current time that the assertion would be valid. For example, if skewTime is 10, then assertion would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all.

signAssertion Option to sign portions of assertion when Citrix ADC IDP sends one. Based on the user selection, either Assertion or Response or Both or none can be signed

signatureService Name of the service in cloud used to sign the data

devno count stateflag

rm vpn samlSSOProfile

Deletes an existing saml single sign-on traffic profile.

Synopsis

rm vpn samlSSOProfile <name>

Arguments

name Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

add vpn samlSSOProfile

Creates a SAML single sign-on profile. This profile is employed in triggering saml assertion to a target service based on traffic profile.

Synopsis

add vpn samlSSOProfile <name> -assertionConsumerServiceURL <URL> [-Attribute1 <string> -Attribute1Expr <string>] [-Attribute2 <string> -Attribute2Expr <string>] [-Attribute3 <string> -Attribute3Expr <string>] [-Attribute4 <string> -Attribute4Expr <string>] [-Attribute5 <string> -Attribute5Expr <string>] [-Attribute6 <string> -Attribute6Expr <string>] [-Attribute7 <string> -Attribute7Expr <string>] [-Attribute8 <string> -Attribute8Expr <string>] [-Attribute9 <string> -Attribute9Expr <string>] [-Attribute10 <string> -Attribute10Expr <string>] [-Attribute11 <string> -Attribute11Expr <string>] [-Attribute12 <string> -Attribute12Expr <string>] [-Attribute13 <string> -Attribute13Expr <string>] [-Attribute14 <string> -Attribute14Expr <string>] [-Attribute15 <string> -Attribute15Expr <string>] [-Attribute16 <string> -Attribute16Expr <string>]

Arguments

name Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period

(.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

samlSigningCertName Name of the signing authority as given in the SAML server's SSL certificate.

assertionConsumerServiceURL URL to which the assertion is to be sent.

relaystateRule Expression to extract relaystate to be sent along with assertion. Evaluation of this expression should return TEXT content. This is typically a target url to which user is redirected after the recipient validates SAML token

samlIssuerName The name to be used in requests sent from Citrix ADC to IdP to uniquely identify Citrix ADC.

signatureAlg Algorithm to be used to sign/verify SAML transactions

Possible values: RSA-SHA1, RSA-SHA256 Default value: RSA-SHA256

digestMethod Algorithm to be used to compute/verify digest for SAML transactions

Possible values: SHA1, SHA256 Default value: SHA256

audience Audience for which assertion sent by IdP is applicable. This is typically entity name or url that represents ServiceProvider

NameIDFormat Format of Name Identifier sent in Assertion.

Possible values: Unspecified, emailAddress, X509SubjectName, WindowsDomainQualifiedName, kerberos, entity, persistent, transient Default value: transient

NameIDExpr Expression that will be evaluated to obtain NameIdentifier to be sent in assertion

Attribute1 Name of attribute1 that needs to be sent in SAML Assertion

Attribute1Expr Expression that will be evaluated to obtain attribute1's value to be sent in Assertion

Attribute1FriendlyName User-Friendly Name of attribute1 that needs to be sent in SAML Assertion

Attribute1Format Format of Attribute1 to be sent in Assertion.

Possible values: URI, Basic

Attribute2 Name of attribute2 that needs to be sent in SAML Assertion

Attribute2Expr Expression that will be evaluated to obtain attribute2's value to be sent in Assertion

Attribute2FriendlyName User-Friendly Name of attribute2 that needs to be sent in SAML Assertion

Attribute2Format Format of Attribute2 to be sent in Assertion.

Possible values: URI, Basic

Attribute3 Name of attribute3 that needs to be sent in SAML Assertion

Attribute3Expr Expression that will be evaluated to obtain attribute3's value to be sent in Assertion

Attribute3FriendlyName User-Friendly Name of attribute3 that needs to be sent in SAML Assertion

Attribute3Format Format of Attribute3 to be sent in Assertion.

Possible values: URI, Basic

Attribute4 Name of attribute4 that needs to be sent in SAML Assertion

Attribute4Expr Expression that will be evaluated to obtain attribute4's value to be sent in Assertion

Attribute4FriendlyName User-Friendly Name of attribute4 that needs to be sent in SAML Assertion

Attribute4Format Format of Attribute4 to be sent in Assertion.

Possible values: URI, Basic

Attribute5 Name of attribute5 that needs to be sent in SAML Assertion

Attribute5Expr Expression that will be evaluated to obtain attribute5's value to be sent in Assertion

Attribute5FriendlyName User-Friendly Name of attribute5 that needs to be sent in SAML Assertion

Attribute5Format Format of Attribute5 to be sent in Assertion.

Possible values: URI, Basic

Attribute6 Name of attribute6 that needs to be sent in SAML Assertion

Attribute6Expr Expression that will be evaluated to obtain attribute6's value to be sent in Assertion

Attribute6FriendlyName User-Friendly Name of attribute6 that needs to be sent in SAML Assertion

Attribute6Format Format of Attribute6 to be sent in Assertion.

Possible values: URI, Basic

Attribute7 Name of attribute7 that needs to be sent in SAML Assertion

Attribute7Expr Expression that will be evaluated to obtain attribute7's value to be sent in Assertion

Attribute7FriendlyName User-Friendly Name of attribute7 that needs to be sent in SAML Assertion

Attribute7Format Format of Attribute7 to be sent in Assertion.

Possible values: URI, Basic

Attribute8 Name of attribute8 that needs to be sent in SAML Assertion

Attribute8Expr Expression that will be evaluated to obtain attribute8's value to be sent in Assertion

Attribute8FriendlyName User-Friendly Name of attribute8 that needs to be sent in SAML Assertion

Attribute8Format Format of Attribute8 to be sent in Assertion.

Possible values: URI, Basic

Attribute9 Name of attribute9 that needs to be sent in SAML Assertion

Attribute9Expr Expression that will be evaluated to obtain attribute9's value to be sent in Assertion

Attribute9FriendlyName User-Friendly Name of attribute9 that needs to be sent in SAML Assertion

Attribute9Format Format of Attribute9 to be sent in Assertion.

Possible values: URI, Basic

Attribute10 Name of attribute10 that needs to be sent in SAML Assertion

Attribute10Expr Expression that will be evaluated to obtain attribute10's value to be sent in Assertion

Attribute10FriendlyName User-Friendly Name of attribute10 that needs to be sent in SAML Assertion

Attribute10Format Format of Attribute10 to be sent in Assertion.

Possible values: URI, Basic

Attribute11 Name of attribute11 that needs to be sent in SAML Assertion

Attribute11Expr Expression that will be evaluated to obtain attribute11's value to be sent in Assertion

Attribute11FriendlyName User-Friendly Name of attribute11 that needs to be sent in SAML Assertion

Attribute11Format Format of Attribute11 to be sent in Assertion.

Possible values: URI, Basic

Attribute12 Name of attribute12 that needs to be sent in SAML Assertion

Attribute12Expr Expression that will be evaluated to obtain attribute12's value to be sent in Assertion

Attribute12FriendlyName User-Friendly Name of attribute12 that needs to be sent in SAML Assertion

Attribute12Format Format of Attribute12 to be sent in Assertion.

Possible values: URI, Basic

Attribute13 Name of attribute13 that needs to be sent in SAML Assertion

Attribute13Expr Expression that will be evaluated to obtain attribute13's value to be sent in Assertion

Attribute13FriendlyName User-Friendly Name of attribute13 that needs to be sent in SAML Assertion

Attribute13Format Format of Attribute13 to be sent in Assertion.

Possible values: URI, Basic

Attribute14 Name of attribute14 that needs to be sent in SAML Assertion

Attribute14Expr Expression that will be evaluated to obtain attribute14's value to be sent in Assertion

Attribute14FriendlyName User-Friendly Name of attribute14 that needs to be sent in SAML Assertion

Attribute14Format Format of Attribute14 to be sent in Assertion.

Possible values: URI, Basic

Attribute15 Name of attribute15 that needs to be sent in SAML Assertion

Attribute15Expr Expression that will be evaluated to obtain attribute15's value to be sent in Assertion

Attribute15FriendlyName User-Friendly Name of attribute15 that needs to be sent in SAML Assertion

Attribute15Format Format of Attribute15 to be sent in Assertion.

Possible values: URI, Basic

Attribute16 Name of attribute16 that needs to be sent in SAML Assertion

Attribute16Expr Expression that will be evaluated to obtain attribute16's value to be sent in Assertion

Attribute16FriendlyName User-Friendly Name of attribute16 that needs to be sent in SAML Assertion

Attribute16Format Format of Attribute16 to be sent in Assertion.

Possible values: URI, Basic

encryptAssertion Option to encrypt assertion when Citrix ADC sends one.

Possible values: ON, OFF Default value: OFF

samlSPCertName Name of the SSL certificate of peer/receving party using which Assertion is encrypted.

encryptionAlgorithm Algorithm to be used to encrypt SAML assertion

Possible values: DES3, AES128, AES192, AES256 Default value: AES256

skewTime This option specifies the number of minutes on either side of current time that the assertion would be valid. For example, if skewTime is 10, then assertion would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all. Default value: 5

signAssertion Option to sign portions of assertion when Citrix ADC IDP sends one. Based on the user selection, either Assertion or Response or Both or none can be signed

Possible values: NONE, ASSERTION, RESPONSE, BOTH Default value: ASSERTION

signatureService Name of the service in cloud used to sign the data

unset vpn samlSSOProfile

Use this command to remove vpn samlSSOProfile settings.Refer to the set vpn samlSSOProfile command for meanings of the arguments.

Synopsis

unset vpn samlSSOProfile <name>

set vpn samlSSOProfile

Modifies the specified attributes of a saml single sign-on traffic profile.

Synopsis

set vpn samlSSOProfile <name> [-Attribute1 <string> -Attribute1Expr <string>] [-Attribute2 <string> -Attribute2Expr <string>] [-Attribute3 <string> -Attribute3Expr <string>] [-Attribute4 <string> -Attribute4Expr <string>] [-Attribute5 <string> -Attribute5Expr <string>] [-Attribute6 <string> -Attribute6Expr <string>] [-Attribute7 <string> -Attribute7Expr <string>] [-Attribute8 <string> -Attribute8Expr <string>] [-Attribute9 <string> -Attribute9Expr <string>] [-Attribute10 <string> -Attribute10Expr <string>] [-Attribute11 <string> -Attribute11Expr <string>] [-Attribute12 <string> -Attribute12Expr <string>] [-Attribute13 <string> -Attribute13Expr <string>] [-Attribute14 <string> -Attribute14Expr <string>] [-Attribute15 <string> -Attribute15Expr <string>] [-Attribute16 <string> -Attribute16Expr <string>]

Arguments

name Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period

(.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

samlSigningCertName Name of the signing authority as given in the SAML server's SSL certificate.

assertionConsumerServiceURL URL to which the assertion is to be sent.

samlIssuerName The name to be used in requests sent from Citrix ADC to IdP to uniquely identify Citrix ADC.

relaystateRule Expression to extract relaystate to be sent along with assertion. Evaluation of this expression should return TEXT content. This is typically a target url to which user is redirected after the recipient validates SAML token

signatureAlg Algorithm to be used to sign/verify SAML transactions

Possible values: RSA-SHA1, RSA-SHA256 Default value: RSA-SHA256

digestMethod Algorithm to be used to compute/verify digest for SAML transactions

Possible values: SHA1, SHA256 Default value: SHA256

audience Audience for which assertion sent by IdP is applicable. This is typically entity name or url that represents ServiceProvider

NameIDFormat Format of Name Identifier sent in Assertion.

Possible values: Unspecified, emailAddress, X509SubjectName, WindowsDomainQualifiedName, kerberos, entity, persistent, transient Default value: transient

NameIDExpr Expression that will be evaluated to obtain NameIdentifier to be sent in assertion

Attribute1 Name of attribute1 that needs to be sent in SAML Assertion

Attribute1Expr Expression that will be evaluated to obtain attribute1's value to be sent in Assertion

Attribute1FriendlyName User-Friendly Name of attribute1 that needs to be sent in SAML Assertion

Attribute1Format Format of Attribute1 to be sent in Assertion.

Possible values: URI, Basic

Attribute2 Name of attribute2 that needs to be sent in SAML Assertion

Attribute2Expr Expression that will be evaluated to obtain attribute2's value to be sent in Assertion

Attribute2FriendlyName User-Friendly Name of attribute2 that needs to be sent in SAML Assertion

Attribute2Format Format of Attribute2 to be sent in Assertion.

Possible values: URI, Basic

Attribute3 Name of attribute3 that needs to be sent in SAML Assertion

Attribute3Expr Expression that will be evaluated to obtain attribute3's value to be sent in Assertion

Attribute3FriendlyName User-Friendly Name of attribute3 that needs to be sent in SAML Assertion

Attribute3Format Format of Attribute3 to be sent in Assertion.

Possible values: URI, Basic

Attribute4 Name of attribute4 that needs to be sent in SAML Assertion

Attribute4Expr Expression that will be evaluated to obtain attribute4's value to be sent in Assertion

Attribute4FriendlyName User-Friendly Name of attribute4 that needs to be sent in SAML Assertion

Attribute4Format Format of Attribute4 to be sent in Assertion.

Possible values: URI, Basic

Attribute5 Name of attribute5 that needs to be sent in SAML Assertion

Attribute5Expr Expression that will be evaluated to obtain attribute5's value to be sent in Assertion

Attribute5FriendlyName User-Friendly Name of attribute5 that needs to be sent in SAML Assertion

Attribute5Format Format of Attribute5 to be sent in Assertion.

Possible values: URI, Basic

Attribute6 Name of attribute6 that needs to be sent in SAML Assertion

Attribute6Expr Expression that will be evaluated to obtain attribute6's value to be sent in Assertion

Attribute6FriendlyName User-Friendly Name of attribute6 that needs to be sent in SAML Assertion

Attribute6Format Format of Attribute6 to be sent in Assertion.

Possible values: URI, Basic

Attribute7 Name of attribute7 that needs to be sent in SAML Assertion

Attribute7Expr Expression that will be evaluated to obtain attribute7's value to be sent in Assertion

Attribute7FriendlyName User-Friendly Name of attribute7 that needs to be sent in SAML Assertion

Attribute7Format Format of Attribute7 to be sent in Assertion.

Possible values: URI, Basic

Attribute8 Name of attribute8 that needs to be sent in SAML Assertion

Attribute8Expr Expression that will be evaluated to obtain attribute8's value to be sent in Assertion

Attribute8FriendlyName User-Friendly Name of attribute8 that needs to be sent in SAML Assertion

Attribute8Format Format of Attribute8 to be sent in Assertion.

Possible values: URI, Basic

Attribute9 Name of attribute9 that needs to be sent in SAML Assertion

Attribute9Expr Expression that will be evaluated to obtain attribute9's value to be sent in Assertion

Attribute9FriendlyName User-Friendly Name of attribute9 that needs to be sent in SAML Assertion

Attribute9Format Format of Attribute9 to be sent in Assertion.

Possible values: URI, Basic

Attribute10 Name of attribute10 that needs to be sent in SAML Assertion

Attribute10Expr Expression that will be evaluated to obtain attribute10's value to be sent in Assertion

Attribute10FriendlyName User-Friendly Name of attribute10 that needs to be sent in SAML Assertion

Attribute10Format Format of Attribute10 to be sent in Assertion.

Possible values: URI, Basic

Attribute11 Name of attribute11 that needs to be sent in SAML Assertion

Attribute11Expr Expression that will be evaluated to obtain attribute11's value to be sent in Assertion

Attribute11FriendlyName User-Friendly Name of attribute11 that needs to be sent in SAML Assertion

Attribute11Format Format of Attribute11 to be sent in Assertion.

Possible values: URI, Basic

Attribute12 Name of attribute12 that needs to be sent in SAML Assertion

Attribute12Expr Expression that will be evaluated to obtain attribute12's value to be sent in Assertion

Attribute12FriendlyName User-Friendly Name of attribute12 that needs to be sent in SAML Assertion

Attribute12Format Format of Attribute12 to be sent in Assertion.

Possible values: URI, Basic

Attribute13 Name of attribute13 that needs to be sent in SAML Assertion

Attribute13Expr Expression that will be evaluated to obtain attribute13's value to be sent in Assertion

Attribute13FriendlyName User-Friendly Name of attribute13 that needs to be sent in SAML Assertion

Attribute13Format Format of Attribute13 to be sent in Assertion.

Possible values: URI, Basic

Attribute14 Name of attribute14 that needs to be sent in SAML Assertion

Attribute14Expr Expression that will be evaluated to obtain attribute14's value to be sent in Assertion

Attribute14FriendlyName User-Friendly Name of attribute14 that needs to be sent in SAML Assertion

Attribute14Format Format of Attribute14 to be sent in Assertion.

Possible values: URI, Basic

Attribute15 Name of attribute15 that needs to be sent in SAML Assertion

Attribute15Expr Expression that will be evaluated to obtain attribute15's value to be sent in Assertion

Attribute15FriendlyName User-Friendly Name of attribute15 that needs to be sent in SAML Assertion

Attribute15Format Format of Attribute15 to be sent in Assertion.

Possible values: URI, Basic

Attribute16 Name of attribute16 that needs to be sent in SAML Assertion

Attribute16Expr Expression that will be evaluated to obtain attribute16's value to be sent in Assertion

Attribute16FriendlyName User-Friendly Name of attribute16 that needs to be sent in SAML Assertion

Attribute16Format Format of Attribute16 to be sent in Assertion.

Possible values: URI, Basic

encryptAssertion Option to encrypt assertion when Citrix ADC sends one.

Possible values: ON, OFF Default value: OFF

samlSPCertName Name of the SSL certificate of peer/receving party using which Assertion is encrypted.

encryptionAlgorithm Algorithm to be used to encrypt SAML assertion

Possible values: DES3, AES128, AES192, AES256 Default value: AES256

skewTime This option specifies the number of minutes on either side of current time that the assertion would be valid. For example, if skewTime is 10, then assertion would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all. Default value: 5

signAssertion Option to sign portions of assertion when Citrix ADC IDP sends one. Based on the user selection, either Assertion or Response or Both or none can be signed

Possible values: NONE, ASSERTION, RESPONSE, BOTH Default value: ASSERTION

signatureService Name of the service in cloud used to sign the data

vpn-sessionAction

The following operations can be performed on "vpn-sessionAction":

set| unset| rm| show| add|

set vpn sessionAction

Modifies an action that was previously added to a session policy that is applied to a user session if the policy expression conditions are met.

Synopsis

set vpn sessionAction <name> [-clientSecurity <expression>] [-wihome <URL>]

Arguments

name The name of the vpn session action.

userAccounting Name of RADIUS Policy to use for user accounting

httpPort Destination port numbers other than port 80, added as a comma-separated list. Traffic to these ports is processed as HTTP traffic, which allows functionality, such as HTTP authorization and single sign-on to a web application to work. Minimum value: 1

winsIP The WINS server ip address.

dnsVserverName Name of the DNS virtual server for the user session.

splitDns Route the DNS requests to the local DNS server configured on the user device, or Citrix Gateway (remote), or both.

Possible values: LOCAL, REMOTE, BOTH

sessTimeout Number of minutes after which the session times out. Minimum value: 1

clientSecurity Specify the client security check for the user device to permit a Citrix Gateway session. The web address or IP address is not included in the expression for the client security check.

clientSecurityGroup The client security group that will be assigned on failure of the client security check. Users can in general be organized into Groups. In this case, the Client Security Group may have a more restrictive security policy.

clientSecurityMessage The client security message that will be displayed on failure of the client security check.

clientSecurityLog Set the logging of client security checks.

Possible values: ON, OFF

splitTunnel Send, through the tunnel, traffic only for intranet applications that are defined in Citrix Gateway. Route all other traffic directly to the Internet. The OFF setting routes all traffic through Citrix Gateway. With the REVERSE setting, intranet applications define the network traffic that is not intercepted. All network traffic directed to internal IP addresses bypasses the VPN tunnel, while other traffic goes through Citrix Gateway. Reverse split tunneling can be used to log all non-local LAN traffic. For example, if users have a home network and are logged on through the Citrix Gateway Plug-in, network traffic destined to a printer or another device within the home network is not intercepted.

Possible values: ON, OFF, REVERSE

localLanAccess Set local LAN access. If split tunneling is OFF, and you set local LAN access to ON, the local client can route traffic to its local interface. When the local area network switch is specified, this combination of switches is useful. The client can allow local LAN access to devices that commonly have non-routable addresses, such as local printers or local file servers.

Possible values: ON, OFF, FORCED

rfc1918 As defined in the local area network, allow only the following local area network addresses to bypass the VPN tunnel when the local LAN access feature is enabled:

- 10..*,
- 172.16..,

- 192.168..

Possible values: ON, OFF

killConnections Specify whether the Citrix Gateway Plug-in should disconnect all preexisting connections, such as the connections existing before the user logged on to Citrix Gateway, and prevent new incoming connections on the Citrix Gateway Plug-in for Windows and MAC when the user is connected to Citrix Gateway and split tunneling is disabled.

Possible values: ON, OFF

transparentInterception Allow access to network resources by using a single IP address and subnet mask or a range of IP addresses. The OFF setting sets the mode to proxy, in which you configure destination and source IP addresses and port numbers. If you are using the Citrix Gateway Plug-in for Windows, set this parameter to ON, in which the mode is set to transparent. If you are using the Citrix Gateway Plug-in for Java, set this parameter to OFF.

Possible values: ON, OFF

defaultAuthorizationAction Specify the network resources that users have access to when they log on to the internal network. The default setting for authorization is to deny access to all network resources. Citrix recommends using the default global setting and then creating authorization policies to define the network resources users can access. If you set the default authorization policy to DENY, you must explicitly authorize access to any network resource, which improves security.

Possible values: ALLOW, DENY

authorizationGroup Comma-separated list of groups in which the user is placed when none of the groups that the user is a part of is configured on Citrix Gateway. The authorization policy can be bound to these groups to control access to the resources.

Smartgroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

clientIdleTimeout Time, in minutes, after which to time out the user session if Citrix Gateway does not detect mouse or keyboard activity. Minimum value: 1 Maximum value: 9999

proxy Set options to apply proxy for accessing the internal resources. Available settings function as follows:

- BROWSER - Proxy settings are configured only in Internet Explorer and Firefox browsers.

- NS - Proxy settings are configured on the Citrix ADC.
- OFF - Proxy settings are not configured.

Possible values: BROWSER, NS, OFF

allProtocolProxy IP address of the proxy server to use for all protocols supported by Citrix Gateway.

httpProxy IP address of the proxy server to be used for HTTP access for all subsequent connections to the internal network.

ftpProxy IP address of the proxy server to be used for FTP access for all subsequent connections to the internal network.

socksProxy IP address of the proxy server to be used for SOCKS access for all subsequent connections to the internal network.

gopherProxy IP address of the proxy server to be used for GOPHER access for all subsequent connections to the internal network.

sslProxy IP address of the proxy server to be used for SSL access for all subsequent connections to the internal network.

proxyException Proxy exception string that will be configured in the browser for bypassing the previously configured proxies. Allowed only if proxy type is Browser.

proxyLocalBypass Bypass proxy server for local addresses option in Internet Explorer and Firefox proxy server settings.

Possible values: ENABLED, DISABLED

clientCleanupPrompt Prompt for client-side cache clean-up when a client-initiated session closes.

Possible values: ON, OFF

forceCleanup Force cache clean-up when the user closes a session. You can specify all, none, or any combination of the client-side items.

clientConfiguration Allow users to change client Debug logging level in Configuration tab of the Citrix Gateway Plug-in for Windows.

SSO Set single sign-on (SSO) for the session. When the user accesses a server, the user's logon credentials are passed to the server for authentication. NOTE : This configuration does not honor the following authentication types for security reason. BASIC, DIGEST, and NTLM (without

Negotiate NTLM2 Key or Negotiate Sign Flag). Use VPN TrafficAction to configure SSO for these authentication types.

Possible values: ON, OFF

ssoCredential Specify whether to use the primary or secondary authentication credentials for single sign-on to the server.

Possible values: PRIMARY, SECONDARY

windowsAutoLogon Enable or disable the Windows Auto Logon for the session. If a VPN session is established after this setting is enabled, the user is automatically logged on by using Windows credentials after the system is restarted.

Possible values: ON, OFF

useMIP Enable or disable the use of a unique IP address alias, or a mapped IP address, as the client IP address for each client session. Allow Citrix Gateway to use the mapped IP address as an intranet IP address when all other IP addresses are not available. When IP pooling is configured and the mapped IP is used as an intranet IP address, the mapped IP address is used when an intranet IP address cannot be assigned.

Possible values: NS, OFF

useIIP Define IP address pool options. Available settings function as follows:

- SPILLOVER - When an address pool is configured and the mapped IP is used as an intranet IP address, the mapped IP address is used when an intranet IP address cannot be assigned.
- NOSPILLOVER - When intranet IP addresses are enabled and the mapped IP address is not used, the Transfer Login page appears for users who have used all available intranet IP addresses.
- OFF - Address pool is not configured.

Possible values: NOSPILLOVER, SPILLOVER, OFF

loginScript Path to the logon script that is run when a session is established. Separate multiple scripts by using comma. A "$" in the path signifies that the word following the "$" is an environment variable.

logoutScript Path to the logout script. Separate multiple scripts by using comma. A "$" in the path signifies that the word following the "$" is an environment variable.

homePage Web address of the home page that appears when users log on. Otherwise, users receive the default home page for Citrix Gateway, which is the Access Interface.

icaProxy Enable ICA proxy to configure secure Internet access to servers running Citrix XenApp or XenDesktop by using Citrix Receiver instead of the Citrix Gateway Plug-in.

Possible values: ON, OFF Default value: OFF

wihome Web address of the Web Interface server, such as http://<ipAddress>/Citrix/XenApp, or Receiver for Web, which enumerates the virtualized resources, such as XenApp, XenDesktop, and cloud applications. This web address is used as the home page in ICA proxy mode. If Client Choices is ON, you must configure this setting. Because the user can choose between FullClient and ICAProxy, the user may see a different home page. An Internet web site may appear if the user gets the FullClient option, or a Web Interface site if the user gets the ICAProxy option. If the setting is not configured, the XenApp option does not appear as a client choice.

wihomeAddressType Type of the wihome address(IPV4/V6)

Possible values: IPV4, IPV6

citrixReceiverHome Web address for the Citrix Receiver home page. Configure Citrix Gateway so that when users log on to the appliance, the Citrix Gateway Plug-in opens a web browser that allows single sign-on to the Citrix Receiver home page.

wiPortalMode Layout on the Access Interface. The COMPACT value indicates the use of small icons.

Possible values: NORMAL, COMPACT

ClientChoices Provide users with multiple logon options. With client choices, users have the option of logging on by using the Citrix Gateway Plug-in for Windows, Citrix Gateway Plug-in for Java, the Web Interface, or clientless access from one location. Depending on how Citrix Gateway is configured, users are presented with up to three icons for logon choices. The most common are the Citrix Gateway Plug-in for Windows, Web Interface, and clientless access.

Possible values: ON, OFF

iipDnsSuffix An intranet IP DNS suffix. When a user logs on to Citrix Gateway and is assigned an IP address, a DNS record for the user name and IP address combination is added to the Citrix Gateway DNS cache. You can configure a DNS suffix to append to the user name when the DNS record is added to the cache. You can reach to the host from where the user is logged on by using

the user's name, which can be easier to remember than an IP address. When the user logs off from Citrix Gateway, the record is removed from the DNS cache.

forcedTimeout Force a disconnection from the Citrix Gateway Plug-in with Citrix Gateway after a specified number of minutes. If the session closes, the user must log on again. Minimum value: 1 Maximum value: 65535

forcedTimeoutWarning Number of minutes to warn a user before the user session is disconnected. Minimum value: 1 Maximum value: 255

ntDomain Single sign-on domain to use for single sign-on to applications in the internal network. This setting can be overwritten by the domain that users specify at the time of logon or by the domain that the authentication server returns.

clientlessVpnMode Enable clientless access for web, XenApp or XenDesktop, and FileShare resources without installing the Citrix Gateway Plug-in. Available settings function as follows:

- ON - Allow only clientless access.
- OFF - Allow clientless access after users log on with the Citrix Gateway Plug-in.
- DISABLED - Do not allow clientless access.

Possible values: ON, OFF, DISABLED Default value: OFF

emailHome Web address for the web-based email, such as Outlook Web Access.

clientlessModeUrlEncoding When clientless access is enabled, you can choose to encode the addresses of internal web applications or to leave the address as clear text. Available settings function as follows:

- OPAQUE - Use standard encoding mechanisms to make the domain and protocol part of the resource unclear to users.
- CLEAR - Do not encode the web address and make it visible to users.
- ENCRYPT - Allow the domain and protocol to be encrypted using a session key. When the web address is encrypted, the URL is different for each user session for the same web resource. If users bookmark the encoded web address, save it in the web browser and then log off, they cannot connect to the web address when they log on and use the bookmark. If users save the encrypted bookmark in the Access Interface during their session, the bookmark works each time the user logs on.

Possible values: TRANSPARENT, OPAQUE, ENCRYPT

clientlessPersistentCookie State of persistent cookies in clientless access mode. Persistent cookies are required for accessing certain features of SharePoint, such as opening and editing Microsoft Word, Excel, and PowerPoint documents hosted on the SharePoint server. A persistent cookie remains on the user device and is sent with each HTTP request. Citrix Gateway encrypts the persistent cookie before sending it to the plug-in on the user device, and refreshes the cookie periodically as long as the session exists. The cookie becomes stale if the session ends. Available settings function as follows:

- ALLOW - Enable persistent cookies. Users can open and edit Microsoft documents stored in SharePoint.
- DENY - Disable persistent cookies. Users cannot open and edit Microsoft documents stored in SharePoint.
- PROMPT - Prompt users to allow or deny persistent cookies during the session. Persistent cookies are not required for clientless access if users do not connect to SharePoint.

Possible values: ALLOW, DENY, PROMPT Default value: DENY

allowedLoginGroups Specify groups that have permission to log on to Citrix Gateway. Users who do not belong to this group or groups are denied access even if they have valid credentials.

SecureBrowse Allow users to connect through Citrix Gateway to network resources from iOS and Android mobile devices with Citrix Receiver. Users do not need to establish a full VPN tunnel to access resources in the secure network.

Possible values: ENABLED, DISABLED

storefronturl Web address for StoreFront to be used in this session for enumeration of resources from XenApp or XenDesktop.

sfGatewayAuthType The authentication type configured for the Citrix Gateway on StoreFront.

Possible values: domain, RSA, domainAndRSA, SMS, smartCard, sfAuth, sfAuthAndRSA

kcdAccount The kcd account details to be used in SSO

rdpClientProfileName Name of the RDP profile associated with the vserver.

WindowsPluginUpgrade Option to set plugin upgrade behaviour for Win

Possible values: Always, Essential, Never

MacPluginUpgrade Option to set plugin upgrade behaviour for Mac

Possible values: Always, Essential, Never

LinuxPluginUpgrade Option to set plugin upgrade behaviour for Linux

Possible values: Always, Essential, Never

iconWithReceiver Option to decide whether to show plugin icon along with receiver

Possible values: ON, OFF

alwaysONProfileName Name of the AlwaysON profile associated with the session action. The builtin profile named none can be used to explicitly disable AlwaysON for the session action.

autoProxyUrl URL to auto proxy config file

AdvancedClientlessVpnMode Option to enable/disable Advanced ClientlessVpnMode. Additionaly, it can be set to STRICT to block Classic ClientlessVpnMode while in AdvancedClientlessMode.

Possible values: ENABLED, DISABLED, STRICT Default value: DISABLED

pcoipProfileName Name of the PCOIP profile associated with the session action. The builtin profile named none can be used to explicitly disable PCOIP for the session action.

fqdnSpoofedIP Spoofed IP address range that can be used by client for FQDN based split tunneling

netmask The netmask for the spoofed ip address

unset vpn sessionAction

Use this command to remove vpn sessionAction settings.Refer to the set vpn sessionAction command for meanings of the arguments.

Synopsis

unset vpn sessionAction <name>

rm vpn sessionAction

Removes an action that was previously added to a session policy.

Synopsis

rm vpn sessionAction <name>

Arguments

name Name of the action to remove.

show vpn sessionAction

Displays a session action that is applied to a user session if the policy expression conditions are met.

Synopsis

show vpn sessionAction

Arguments

name Name of the session action to display.

Output

userAccounting RADIUS policy to use for user accounting

httpPort The HTTP port for this session action

winsIP The WINS server IP address for this session action.

dnsVserverName The name of the DNS vserver configured by the session action.

splitDns The VPN client SplitDns state.

sessTimeout The session timeout, in minutes, set by the action.

clientSecurity The client security check string being applied. This is in the form of an expression. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

clientSecurityGroup The client security group that will be assigned on failure of the client security check. Users can in general be organized into Groups. In this case, the Client Security Group may have a more restrictive security policy.

clientSecurityMessage The client security message that will be displayed on failure of the client security check.

clientSecurityLog Set the logging of client security checks.

splitTunnel Send, through the tunnel, traffic only for intranet applications that are defined in Citrix Gateway. Route all other traffic directly to the Internet. The OFF setting routes all traffic through Citrix Gateway. With the REVERSE setting, intranet applications define the network traffic that is not intercepted. All network traffic directed to internal IP addresses bypasses the VPN tunnel, while other traffic goes through Citrix Gateway. Reverse split tunneling can be used to log all non-local LAN traffic. For example, if users have a home network and are logged on through the Citrix Gateway Plug-in, network traffic destined to a printer or another device within the home network is not intercepted.

localLanAccess Set local LAN access. If split tunneling is OFF, and you set local LAN access to ON, the local client can route traffic to its local interface. When the local area network switch is specified, this combination of switches is useful. The client can allow local LAN access to devices that commonly have non-routable addresses, such as local printers or local file servers.

rfc1918 As defined in the local area network, allow only the following local area network addresses to bypass the VPN tunnel when the local LAN access feature is enabled:

- 10...*,
- 172.16..,
- 192.168..

spoofIIP IP address that the intranet application uses to route the connection through the virtual adapter.

killConnections Specify whether the Citrix Gateway Plug-in should disconnect all preexisting connections, such as the connections existing before the user logged on to Citrix Gateway, and prevent new incoming connections on the Citrix Gateway Plug-in for Windows and MAC when the user is connected to Citrix Gateway and split tunneling is disabled.

transparentInterception Allow access to network resources by using a single IP address and subnet mask or a range of IP addresses. The OFF setting sets the mode to proxy, in which you configure destination and source IP addresses and port numbers. If you are using the Citrix Gateway Plug-in for Windows, set this parameter to ON, in which the mode is set to transparent. If you are using the Citrix Gateway Plug-in for Java, set this parameter to OFF.

windowsClientType Windows client type, e.g. Agent or ActiveX

defaultAuthorizationAction The Authorization Action, e.g. allow or deny

authorizationGroup The authorization group applied to client sessions.

Smartgroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups.

clientIdleTimeout The client idle timeout, in minutes.

clientIdleTimeoutWarning The time after which the client gets a timeout warning, in minutes.

proxy The state of proxy configuration for the session.

allProtocolProxy The address set for all proxies.

httpProxy The HTTP proxy IP address.

ftpProxy The FTP proxy IP address.

socksProxy IP address of the proxy server to be used for SOCKS access for all subsequent connections to the internal network.

gopherProxy The Gopher proxy IP address.

sslProxy The HTTPS proxy IP address.

proxyException Proxy exception string that will be configured in the browser for bypassing the previously configured proxies. Allowed only if proxy type is Browser.

proxyLocalBypass Bypass proxy server for local addresses option in Internet Explorer and Firefox proxy server settings.

clientCleanupPrompt Prompt for client-side cache clean-up when a client-initiated session closes.

forceCleanup Force cache clean-up when the user closes a session. You can specify all, none, or any combination of the client-side items.

clientOptions List of configured buttons(and/or menu options in the docked client) in the Windows VPN client.

clientConfiguration List of configured tabs in the Windows VPN client.

SSO Whether or not Single Sign-On is used for this session.

ssoCredential Specify whether to use the primary or secondary authentication credentials for single sign-on to the server.

windowsAutoLogon Whether or not Windows Auto Logon is enabled for this session.

useMIP Whether or not a Mapped IP address is used for the session

useIIP Define IP address pool options. Available settings function as follows:

- SPILLOVER - When an address pool is configured and the mapped IP is used as an intranet IP address, the mapped IP address is used when an intranet IP address cannot be assigned.
- NOSPILLOVER - When intranet IP addresses are enabled and the mapped IP address is not used, the Transfer Login page appears for users who have used all available intranet IP addresses.
- OFF - Address pool is not configured.

clientDebug Trace level on the Windows VPN Client.

loginScript Path to the logon script that is run when a session is established. Separate multiple scripts by using comma. A "$" in the path signifies that the word following the "$" is an environment variable.

logoutScript Path to the logout script. Separate multiple scripts by using comma. A "$" in the path signifies that the word following the "$" is an environment variable.

homePage The client home page.

icaProxy Enable ICA proxy to configure secure Internet access to servers running Citrix XenApp or XenDesktop by using Citrix Receiver instead of the Citrix Gateway Plug-in.

wihome Web address of the Web Interface server, such as http://<ipAddress>/Citrix/XenApp, or Receiver for Web, which enumerates the virtualized resources, such as XenApp, XenDesktop, and cloud applications. This web address is used as the home page in ICA proxy mode. If Client Choices is ON, you must configure this setting. Because the user can choose between FullClient and ICAProxy, the user may see a different home page. An Internet web site may appear if the user gets the FullClient option, or a Web Interface site if the user gets the ICAProxy option. If the setting is not configured, the XenApp option does not appear as a client choice.

wihomeAddressType Type of the wihome address(IPV4/V6)

citrixReceiverHome Web address for the Citrix Receiver home page. Configure Citrix Gateway so that when users log on to the appliance, the Citrix Gateway Plug-in opens a web browser that allows single sign-on to the Citrix Receiver home page.

wiPortalMode Layout on the Access Interface. The COMPACT value indicates the use of small icons.

ClientChoices Provide users with multiple logon options. With client choices, users have the option of logging on by using the Citrix Gateway Plug-in for Windows, Citrix Gateway Plug-in for Java, the Web Interface, or clientless access from one location. Depending on how Citrix Gateway is configured, users are presented with up to three icons for logon choices. The most common are the Citrix Gateway Plug-in for Windows, Web Interface, and clientless access.

epaClientType Choose between two types of End point Windows Client a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed b) Activex Control - ActiveX control run by Microsoft Internet Explorer.

iipDnsSuffix The IntranetIP DNS suffix.

forcedTimeout Force a disconnection from the Citrix Gateway Plug-in with Citrix Gateway after a specified number of minutes. If the session closes, the user must log on again.

forcedTimeoutWarning Number of minutes to warn a user before the user session is disconnected.

ntDomain Single sign-on domain to use for single sign-on to applications in the internal network. This setting can be overwritten by the domain that users specify at the time of logon or by the domain that the authentication server returns.

clientlessVpnMode Whether clientlessVPN is available to the session.

clientlessModeUrlEncoding URL encoding used in clientless mode.

clientlessPersistentCookie State of persistent cookies in clientless access mode. Persistent cookies are required for accessing certain features of SharePoint, such as opening and editing Microsoft Word, Excel, and PowerPoint documents hosted on the SharePoint server. A persistent cookie remains on the user device and is sent with each HTTP request. Citrix Gateway encrypts the persistent cookie before sending it to the plug-in on the user device, and refreshes the cookie periodically as long as the session exists. The cookie becomes stale if the session ends. Available settings function as follows:

- ALLOW - Enable persistent cookies. Users can open and edit Microsoft documents stored in SharePoint.
- DENY - Disable persistent cookies. Users cannot open and edit Microsoft documents stored in SharePoint.
- PROMPT - Prompt users to allow or deny persistent cookies during the session. Persistent cookies are not required for clientless access if users do not connect to SharePoint.

emailHome The EMail home for the portal

stateflag allowedLoginGroups Specify groups that have permission to log on to Citrix Gateway. Users who do not belong to this group or groups are denied access even if they have valid credentials.

SecureBrowse Allow users to connect through Citrix Gateway to network resources from iOS and Android mobile devices with Citrix Receiver. Users do not need to establish a full VPN tunnel to access resources in the secure network.

storefronturl Web address for StoreFront to be used in this session for enumeration of resources from XenApp or XenDesktop.

sfGatewayAuthType The authentication type configured for the Citrix Gateway on StoreFront.

kcdAccount The kcd account details to be used in SSO

rdpClientProfileName Name of the RDP profile associated with the vserver.

builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

WindowsPluginUpgrade Option to set plugin upgrade behaviour for Win

MacPluginUpgrade Option to set plugin upgrade behaviour for Mac

LinuxPluginUpgrade Option to set plugin upgrade behaviour for Linux

iconWithReceiver Option to decide whether to show plugin icon along with receiver

alwaysONProfileName Name of the AlwaysON profile associated with the session action. The builtin profile named none can be used to explicitly disable AlwaysON for the session action.

autoProxyUrl URL to auto proxy config file

AdvancedClientlessVpnMode Option to enable/disable Advanced ClientlessVpnMode. Additionaly, it can be set to STRICT to block Classic ClientlessVpnMode while in AdvancedClientlessMode.

pcoipProfileName Name of the PCOIP profile associated with the session action. The builtin profile named none can be used to explicitly disable PCOIP for the session action.

fqdnSpoofedIP Spoofed IP address range that can be used by client for FQDN based split tunneling

netmask The netmask for the spoofed ip address

devno count

add vpn sessionAction

Adds a session profile (action) to bind to a session policy that is applied to a user session if the policy expression conditions are met.

Synopsis

add vpn sessionAction <name> [-clientSecurity <expression>] [-wihome <URL>]

Arguments

name Name for the Citrix Gateway profile (action). Must begin with an ASCII alphabetic or underscore (_) character, and must consist only of ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the profile is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

userAccounting The name of the radiusPolicy to use for RADIUS user accounting info on the session.

httpPort Destination port numbers other than port 80, added as a comma-separated list. Traffic to these ports is processed as HTTP traffic, which allows functionality, such as HTTP authorization and single sign-on to a web application to work. Minimum value: 1

winsIP WINS server IP address to add to Citrix Gateway for name resolution.

dnsVserverName Name of the DNS virtual server for the user session.

splitDns Route the DNS requests to the local DNS server configured on the user device, or Citrix Gateway (remote), or both.

Possible values: LOCAL, REMOTE, BOTH

sessTimeout Number of minutes after which the session times out. Minimum value: 1

clientSecurity Specify the client security check for the user device to permit a Citrix Gateway session. The web address or IP address is not included in the expression for the client security check.

clientSecurityGroup The client security group that will be assigned on failure of the client security check. Users can in general be organized into Groups. In this case, the Client Security Group may have a more restrictive security policy.

clientSecurityMessage The client security message that will be displayed on failure of the client security check.

clientSecurityLog Set the logging of client security checks.

Possible values: ON, OFF

splitTunnel Send, through the tunnel, traffic only for intranet applications that are defined in Citrix Gateway. Route all other traffic directly to the Internet. The OFF setting routes all traffic through Citrix Gateway. With the REVERSE setting, intranet applications define the network traffic that is not intercepted. All network traffic directed to internal IP addresses bypasses the VPN tunnel, while other traffic goes through Citrix Gateway. Reverse split tunneling can be used to log all non-local LAN traffic. For example, if users have a home network and are logged on through the Citrix Gateway Plug-in, network traffic destined to a printer or another device within the home network is not intercepted.

Possible values: ON, OFF, REVERSE

localLanAccess Set local LAN access. If split tunneling is OFF, and you set local LAN access to ON, the local client can route traffic to its local interface. When the local area network switch is specified, this combination of switches is useful. The client can allow local LAN access to devices that commonly have non-routable addresses, such as local printers or local file servers.

Possible values: ON, OFF, FORCED

rfc1918 As defined in the local area network, allow only the following local area network addresses to bypass the VPN tunnel when the local LAN access feature is enabled:

- 10...*,
- 172.16..,
- 192.168..

Possible values: ON, OFF

killConnections Specify whether the Citrix Gateway Plug-in should disconnect all preexisting connections, such as the connections existing before the user logged on to Citrix Gateway, and prevent new incoming connections on the Citrix Gateway Plug-in for Windows and MAC when the user is connected to Citrix Gateway and split tunneling is disabled.

Possible values: ON, OFF

transparentInterception Allow access to network resources by using a single IP address and subnet mask or a range of IP addresses. The OFF setting sets the mode to proxy, in which you configure destination and source IP addresses and port numbers. If you are using the Citrix Gateway Plug-in for Windows, set this parameter to ON, in which the mode is set to transparent. If you are using the Citrix Gateway Plug-in for Java, set this parameter to OFF.

Possible values: ON, OFF

defaultAuthorizationAction Specify the network resources that users have access to when they log on to the internal network. The default setting for authorization is to deny access to all network resources. Citrix recommends using the default global setting and then creating authorization policies to define the network resources users can access. If you set the default authorization policy to DENY, you must explicitly authorize access to any network resource, which improves security.

Possible values: ALLOW, DENY

authorizationGroup Comma-separated list of groups in which the user is placed when none of the groups that the user is a part of is configured on Citrix Gateway. The authorization policy can be bound to these groups to control access to the resources.

Smartgroup This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum value: 64

clientIdleTimeout Time, in minutes, after which to time out the user session if Citrix Gateway does not detect mouse or keyboard activity. Minimum value: 1 Maximum value: 9999

proxy Set options to apply proxy for accessing the internal resources. Available settings function as follows:

- BROWSER - Proxy settings are configured only in Internet Explorer and Firefox browsers.
- NS - Proxy settings are configured on the Citrix ADC.
- OFF - Proxy settings are not configured.

Possible values: BROWSER, NS, OFF

allProtocolProxy IP address of the proxy server to use for all protocols supported by Citrix Gateway.

httpProxy IP address of the proxy server to be used for HTTP access for all subsequent connections to the internal network.

ftpProxy IP address of the proxy server to be used for FTP access for all subsequent connections to the internal network.

socksProxy IP address of the proxy server to be used for SOCKS access for all subsequent connections to the internal network.

gopherProxy IP address of the proxy server to be used for GOPHER access for all subsequent connections to the internal network.

sslProxy IP address of the proxy server to be used for SSL access for all subsequent connections to the internal network.

proxyException Proxy exception string that will be configured in the browser for bypassing the previously configured proxies. Allowed only if proxy type is Browser.

proxyLocalBypass Bypass proxy server for local addresses option in Internet Explorer and Firefox proxy server settings.

Possible values: ENABLED, DISABLED

clientCleanupPrompt Prompt for client-side cache clean-up when a client-initiated session closes.

Possible values: ON, OFF

forceCleanup Force cache clean-up when the user closes a session. You can specify all, none, or any combination of the client-side items.

clientConfiguration Allow users to change client Debug logging level in Configuration tab of the Citrix Gateway Plug-in for Windows.

SSO Set single sign-on (SSO) for the session. When the user accesses a server, the user's logon credentials are passed to the server for authentication. NOTE : This configuration does not honor the following authentication types for security reason. BASIC, DIGEST, and NTLM (without Negotiate NTLM2 Key or Negotiate Sign Flag). Use VPN TrafficAction to configure SSO for these authentication types.

Possible values: ON, OFF

ssoCredential Specify whether to use the primary or secondary authentication credentials for single sign-on to the server.

Possible values: PRIMARY, SECONDARY

windowsAutoLogon Enable or disable the Windows Auto Logon for the session. If a VPN session is established after this setting is enabled, the user is automatically logged on by using Windows credentials after the system is restarted.

Possible values: ON, OFF

useMIP Enable or disable the use of a unique IP address alias, or a mapped IP address, as the client IP address for each client session. Allow Citrix Gateway to use the mapped IP address as an intranet IP address when all other IP addresses are not available. When IP pooling is configured and the mapped IP is used as an intranet IP address, the mapped IP address is used when an intranet IP address cannot be assigned.

Possible values: NS, OFF

useIIP Define IP address pool options. Available settings function as follows:

- SPILLOVER - When an address pool is configured and the mapped IP is used as an intranet IP address, the mapped IP address is used when an intranet IP address cannot be assigned.
- NOSPILLOVER - When intranet IP addresses are enabled and the mapped IP address is not used, the Transfer Login page appears for users who have used all available intranet IP addresses.
- OFF - Address pool is not configured.

Possible values: NOSPILLOVER, SPILLOVER, OFF

loginScript Path to the logon script that is run when a session is established. Separate multiple scripts by using comma. A "$" in the path signifies that the word following the "$" is an environment variable.

logoutScript Path to the logout script. Separate multiple scripts by using comma. A "$" in the path signifies that the word following the "$" is an environment variable.

homePage Web address of the home page that appears when users log on. Otherwise, users receive the default home page for Citrix Gateway, which is the Access Interface.

icaProxy Enable ICA proxy to configure secure Internet access to servers running Citrix XenApp or XenDesktop by using Citrix Receiver instead of the Citrix Gateway Plug-in.

Possible values: ON, OFF

wihome Web address of the Web Interface server, such as http://<ipAddress>/Citrix/XenApp, or Receiver for Web, which enumerates the virtualized resources, such as XenApp, XenDesktop, and cloud applications. This web address is used as the home page in ICA proxy mode. If Client Choices is ON, you must configure this setting. Because the user can choose between FullClient and ICAProxy, the user may see a different home page. An Internet web site may appear if the user gets the FullClient option, or a Web Interface site if the user gets the ICAProxy option. If the setting is not configured, the XenApp option does not appear as a client choice.

wihomeAddressType Type of the wihome address(IPV4/V6)

Possible values: IPV4, IPV6

citrixReceiverHome Web address for the Citrix Receiver home page. Configure Citrix Gateway so that when users log on to the appliance, the Citrix Gateway Plug-in opens a web browser that allows single sign-on to the Citrix Receiver home page.

wiPortalMode Layout on the Access Interface. The COMPACT value indicates the use of small icons.

Possible values: NORMAL, COMPACT

ClientChoices Provide users with multiple logon options. With client choices, users have the option of logging on by using the Citrix Gateway Plug-in for Windows, Citrix Gateway Plug-in for Java, the Web Interface, or clientless access from one location. Depending on how Citrix Gateway is configured, users are presented with up to three icons for logon choices. The most common are the Citrix Gateway Plug-in for Windows, Web Interface, and clientless access.

Possible values: ON, OFF

iipDnsSuffix An intranet IP DNS suffix. When a user logs on to Citrix Gateway and is assigned an IP address, a DNS record for the user name and IP address combination is added to the Citrix Gateway DNS cache. You can configure a DNS suffix to append to the user name when the DNS record is added to the cache. You can reach to the host from where the user is logged on by using the user's name, which can be easier to remember than an IP address. When the user logs off from Citrix Gateway, the record is removed from the DNS cache.

forcedTimeout Force a disconnection from the Citrix Gateway Plug-in with Citrix Gateway after a specified number of minutes. If the session closes, the user must log on again. Minimum value: 1 Maximum value: 65535

forcedTimeoutWarning Number of minutes to warn a user before the user session is disconnected. Minimum value: 1 Maximum value: 255

ntDomain Single sign-on domain to use for single sign-on to applications in the internal network. This setting can be overwritten by the domain that users specify at the time of logon or by the domain that the authentication server returns.

clientlessVpnMode Enable clientless access for web, XenApp or XenDesktop, and FileShare resources without installing the Citrix Gateway Plug-in. Available settings function as follows:

- ON - Allow only clientless access.
- OFF - Allow clientless access after users log on with the Citrix Gateway Plug-in.
- DISABLED - Do not allow clientless access.

Possible values: ON, OFF, DISABLED

emailHome Web address for the web-based email, such as Outlook Web Access.

clientlessModeUrlEncoding When clientless access is enabled, you can choose to encode the addresses of internal web applications or to leave the address as clear text. Available settings function as follows:

- OPAQUE - Use standard encoding mechanisms to make the domain and protocol part of the resource unclear to users.
- CLEAR - Do not encode the web address and make it visible to users.
- ENCRYPT - Allow the domain and protocol to be encrypted using a session key. When the web address is encrypted, the URL is different for each user session for the same web resource. If users bookmark the encoded web address, save it in the web browser and then log off, they cannot connect to the web address when they log on and use the bookmark. If users save the encrypted bookmark in the Access Interface during their session, the bookmark works each time the user logs on.

Possible values: TRANSPARENT, OPAQUE, ENCRYPT

clientlessPersistentCookie State of persistent cookies in clientless access mode. Persistent cookies are required for accessing certain features of SharePoint, such as opening and editing Microsoft Word, Excel, and PowerPoint documents hosted on the SharePoint server. A persistent cookie remains on the user device and is sent with each HTTP request. Citrix Gateway encrypts the persistent cookie before sending it to the plug-in on the user device, and refreshes the cookie

periodically as long as the session exists. The cookie becomes stale if the session ends. Available settings function as follows:

- ALLOW - Enable persistent cookies. Users can open and edit Microsoft documents stored in SharePoint.
- DENY - Disable persistent cookies. Users cannot open and edit Microsoft documents stored in SharePoint.
- PROMPT - Prompt users to allow or deny persistent cookies during the session. Persistent cookies are not required for clientless access if users do not connect to SharePoint.

Possible values: ALLOW, DENY, PROMPT

allowedLoginGroups Specify groups that have permission to log on to Citrix Gateway. Users who do not belong to this group or groups are denied access even if they have valid credentials.

SecureBrowse Allow users to connect through Citrix Gateway to network resources from iOS and Android mobile devices with Citrix Receiver. Users do not need to establish a full VPN tunnel to access resources in the secure network.

Possible values: ENABLED, DISABLED

storefronturl Web address for StoreFront to be used in this session for enumeration of resources from XenApp or XenDesktop.

sfGatewayAuthType The authentication type configured for the Citrix Gateway on StoreFront.

Possible values: domain, RSA, domainAndRSA, SMS, smartCard, sfAuth, sfAuthAndRSA

kcdAccount The kcd account details to be used in SSO

rdpClientProfileName Name of the RDP profile associated with the vserver.

WindowsPluginUpgrade Option to set plugin upgrade behaviour for Win

Possible values: Always, Essential, Never

MacPluginUpgrade Option to set plugin upgrade behaviour for Mac

Possible values: Always, Essential, Never

LinuxPluginUpgrade Option to set plugin upgrade behaviour for Linux

Possible values: Always, Essential, Never

iconWithReceiver Option to decide whether to show plugin icon along with receiver

Possible values: ON, OFF

alwaysONProfileName Name of the AlwaysON profile associated with the session action. The builtin profile named none can be used to explicitly disable AlwaysON for the session action.

autoProxyUrl URL to auto proxy config file

AdvancedClientlessVpnMode Option to enable/disable Advanced ClientlessVpnMode. Additionaly, it can be set to STRICT to block Classic ClientlessVpnMode while in AdvancedClientlessMode.

Possible values: ENABLED, DISABLED, STRICT Default value: DISABLED

pcoipProfileName Name of the PCOIP profile associated with the session action. The builtin profile named none can be used to explicitly disable PCOIP for the session action.

fqdnSpoofedIP Spoofed IP address range that can be used by client for FQDN based split tunneling

netmask The netmask for the spoofed ip address

vpn-sessionPolicy

The following operations can be performed on "vpn-sessionPolicy":

add| set| show| rm| unset|

add vpn sessionPolicy

Creates a new session policy that, if bound, is applied after the user logs on to Citrix Gateway, and that determines the properties of the user session.

Synopsis

add vpn sessionPolicy <name> <rule> <action>

Arguments

name Name for the new session policy that is applied after the user logs on to Citrix Gateway.

rule Expression, or name of a named expression, specifying the traffic that matches the policy.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Action to be applied by the new session policy if the rule criteria are met.

set vpn sessionPolicy

Modifies the rule or action of a session policy.

Synopsis

set vpn sessionPolicy <name>

Arguments

name Name of the session policy to modify.

rule Expression, or name of a named expression, specifying the traffic that matches the policy.

The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Action to be applied by the new session policy if the rule criteria are met.

show vpn sessionPolicy

Displays a session policy.

Synopsis

show vpn sessionPolicy

Arguments

name Name of the session policy to display.

Output

rule The new rule associated with the policy. Rules are combinations of expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide.

action The new vpn session action the policy is using.

boundTo The entity name to which policy is bound

activePolicy priority bindPolicyType policyType builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

feature The feature to be checked while applying this config

expressionType Type of policy (Classic/Advanced)

hits Number of hits.

piHits Number of hits.

devno count stateflag

rm vpn sessionPolicy

Removes the session policy that is applied after the user logs on to Citrix Gateway.

Synopsis

rm vpn sessionPolicy <name>

Arguments

name Name of the session policy to remove.

unset vpn sessionPolicy

Use this command to remove vpn sessionPolicy settings.Refer to the set vpn sessionPolicy command for meanings of the arguments.

Synopsis

unset vpn sessionPolicy <name>

vpn-sfconfig

The following operations can be performed on "vpn-sfconfig":

show vpn sfconfig

Create a configuration file for a given VPN virtual server, which can be imported by StoreFront.

Synopsis

show vpn sfconfig

Arguments

vServer Name of Gateway virtual server

Output

fileName Path where file was created

devno count stateflag

Example

show vpn sfconfig <vserver name>

vpn-stats

The following operations can be performed on "vpn-stats":

show vpn stats

show vpn stats is an alias for stat vpn

Synopsis

show vpn stats - alias for 'stat vpn'

vpn-storeinfo

The following operations can be performed on "vpn-storeinfo":

show vpn storeinfo

Show the Store Front information summary

Synopsis

show vpn storeinfo -url <URL>

Arguments

url StoreFront URL to be scanned

Output

storeServerStatus Availability of the server for TCP connections

storeServerIsSf Indicates if the server being scanned is running StoreFront.

storeApiSupport Indicates StoreFront API support status

storeList List of available stores return by StoreFront API

storeStatus Availability of the specified StoreFront store

devno count stateflag

Example

show vpn storeinfo -url <url>

vpn-trafficAction

The following operations can be performed on "vpn-trafficAction":

unset| add| show| rm| set|

unset vpn trafficAction

Use this command to remove vpn trafficAction settings.Refer to the set vpn trafficAction command for meanings of the arguments.

Synopsis

unset vpn trafficAction <name>

add vpn trafficAction

Creates an action to be applied by a policy that matches the traffic being processed.

Synopsis

add vpn trafficAction <name> <qual> [(-SSO (ON | OFF)) | -wanscaler (ON | OFF)]

Arguments

name Name for the traffic action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after a traffic action is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').

qual Protocol, either HTTP or TCP, to be used with the action.

Possible values: http, tcp

appTimeout Maximum amount of time, in minutes, a user can stay logged on to the web application. Minimum value: 1 Maximum value: 715827

SSO Provide single sign-on to the web application. NOTE : Authentication mechanisms like Basic-authentication require the user credentials to be sent in plaintext which is not secure if the server is running on HTTP (instead of HTTPS).

Possible values: ON, OFF

HDX Provide hdx proxy to the ICA traffic

Possible values: ON, OFF

formSSOAction Name of the form-based single sign-on profile. Form-based single sign-on allows users to log on one time to all protected applications in your network, instead of requiring them to log on separately to access each one.

fta Specify file type association, which is a list of file extensions that users are allowed to open.

Possible values: ON, OFF

wanscaler Use the Repeater Plug-in to optimize network traffic.

Possible values: ON, OFF

kcdAccount Kerberos constrained delegation account name Default value: "Default"

samlSSOProfile Profile to be used for doing SAML SSO to remote relying party

proxy IP address and Port of the proxy server to be used for HTTP access for this request.

userExpression expression that will be evaluated to obtain username for SingleSignOn Maximum value: 256

passwdExpression expression that will be evaluated to obtain password for SingleSignOn Maximum value: 256

show vpn trafficAction

Displays information about all the configured traffic actions, or displays detailed information about the specified traffic action.

Synopsis

show vpn trafficAction

Arguments

name Name of the traffic policy action for which to display detailed information.

Output

qual The protocol that is set with the action; for example, http or tcp.

appTimeout The application timeout

SSO Whether or not Single Sign On is enabled.

formSSOAction Name of the form-based single sign-on profile. Form-based single sign-on allows users to log on one time to all protected applications in your network, instead of requiring them to log on separately to access each one.

HDX Whether or not HDX Proxy for ICA traffic is enabled.

fta Whether or not file-type association is enabled.

wanscaler Use the Repeater Plug-in to optimize network traffic.

kcdAccount Kerberos constrained delegation account name

samlSSOProfile Profile to be used for doing SAML SSO to remote relying party

proxy IP address and Port of the proxy server to be used for HTTP access for this request.

userExpression expression that will be evaluated to obtain username for SingleSignOn

passwdExpression expression that will be evaluated to obtain password for SingleSignOn

stateflag devno count

rm vpn trafficAction

Removes a previously created traffic policy action.

Synopsis

rm vpn trafficAction <name>

Arguments

name Name of the traffic policy action to remove.

set vpn trafficAction

Modifies a traffic policy action to be applied by the policy if the rule criteria are met.

Synopsis

set vpn trafficAction <name>

Arguments

name Name of the traffic policy action to modify.

appTimeout Maximum amount of time, in minutes, a user can stay logged on to the web application. Minimum value: 1 Maximum value: 715827

SSO Provide single sign-on to the web application. NOTE : Authentication mechanisms like Basic-authentication require the user credentials to be sent in plaintext which is not secure if the server is running on HTTP (instead of HTTPS).

Possible values: ON, OFF

HDX Provide hdx proxy to the ICA traffic

Possible values: ON, OFF

formSSOAction Name of the form-based single sign-on profile. Form-based single sign-on allows users to log on one time to all protected applications in your network, instead of requiring them to log on separately to access each one.

fta Specify file type association, which is a list of file extensions that users are allowed to open.

Possible values: ON, OFF

wanscaler Use the Repeater Plug-in to optimize network traffic.

Possible values: ON, OFF

kcdAccount Kerberos constrained delegation account name Default value: "Default"

samlSSOProfile Profile to be used for doing SAML SSO to remote relying party

proxy IP address and Port of the proxy server to be used for HTTP access for this request.

userExpression expression that will be evaluated to obtain username for SingleSignOn Maximum value: 256

passwdExpression expression that will be evaluated to obtain password for SingleSignOn Maximum value: 256

vpn-trafficPolicy

The following operations can be performed on "vpn-trafficPolicy":

set| unset| rm| show| add|

set vpn trafficPolicy

Modifies the specified parameters of an existing traffic policy.

Synopsis

set vpn trafficPolicy <name>

Arguments

name Name of the traffic policy to modify.

rule Expression, or name of a named expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.

- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Action to apply to traffic that matches the policy.

unset vpn trafficPolicy

Use this command to remove vpn trafficPolicy settings.Refer to the set vpn trafficPolicy command for meanings of the arguments.

Synopsis

unset vpn trafficPolicy <name>

rm vpn trafficPolicy

Removes an existing traffic policy from Citrix Gateway.

Synopsis

rm vpn trafficPolicy <name>

Arguments

name Name of the traffic policy to remove.

show vpn trafficPolicy

Displays information about all Citrix Gateway traffic policies, or detailed information about the specified policy.

Synopsis

show vpn trafficPolicy

Arguments

name Name of the traffic policy for which to display detailed information.

Output

rule The rule used by the vpn traffic policy. Rules are combinations of expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide

action The action to be performed when the rule is matched.

boundTo The entity name to which policy is bound

activePolicy priority bindPolicyType policyType expressionType Type of policy (Classic/ Advanced)

hits Number of hits.

piHits Number of hits.

devno count stateflag

add vpn trafficPolicy

Creates a traffic policy. A traffic policy conditionally sets Citrix Gateway traffic characteristics at run time. For an intranet resource, for example, the traffic policy parameters define the destination IP address, destination port, amount of time a user can stay logged on to the application, and HTTP compression.

Synopsis

add vpn trafficPolicy <name> <rule> <action>

Arguments

name Name for the traffic policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the policy is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy').

rule Expression, or name of a named expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Action to apply to traffic that matches the policy.

vpn-url

The following operations can be performed on "vpn-url":

rm| add| set| show| unset|

rm vpn url

Removes a bookmark link to an internal resource that appears in the Access Interface.

Synopsis

rm vpn url <urlName>

Arguments

urlName Name of the bookmark link to remove.

Example

rm vpn url ggl

add vpn url

Creates a bookmark link to an external or internal resource that appears on the Access Interface, according to type, as a web site link or file share link.

Synopsis

add vpn url <urlName> <linkName> <actualURL>

Arguments

urlName Name of the bookmark link.

linkName Description of the bookmark link. The description appears in the Access Interface.

actualURL Web address for the bookmark link.

vServerName Name of the associated LB/CS vserver

clientlessAccess If clientless access to the resource hosting the link is allowed, also use clientless access for the bookmarked web address in the Secure Client Access based session. Allows single sign-on and other HTTP processing on Citrix Gateway for HTTPS resources.

Possible values: ON, OFF Default value: OFF

comment Any comments associated with the bookmark link.

iconURL URL to fetch icon file for displaying this resource.

ssotype Single sign on type for unified gateway

Possible values: unifiedgateway, selfauth, samlauth

applicationtype The type of application this VPN URL represents. Possible values are CVPN/ SaaS/VPN

Possible values: CVPN, VPN, SaaS

samlSSOProfile Profile to be used for doing SAML SSO

appJson To store the template details in the json format.

Example

add vpn url ggl search www.google.com.

set vpn url

Modifies the specified parameters of a bookmark link to an internal resource that appears in the Access Interface.

Synopsis

set vpn url <urlName>

Arguments

urlName Name of the bookmark link.

linkName Description of the bookmark link. The description appears in the Access Interface.

actualURL Web address for the bookmark link.

vServerName Name of the associated LB/CS vserver

clientlessAccess If clientless access to the resource hosting the link is allowed, also use clientless access for the bookmarked web address in the Secure Client Access based session. Allows single sign-on and other HTTP processing on Citrix Gateway for HTTPS resources.

Possible values: ON, OFF Default value: OFF

comment Any comments associated with the bookmark link.

iconURL URL to fetch icon file for displaying this resource.

ssotype Single sign on type for unified gateway

Possible values: unifiedgateway, selfauth, samlauth

applicationtype The type of application this VPN URL represents. Possible values are CVPN/ SaaS/VPN

Possible values: CVPN, VPN, SaaS

samlSSOProfile Profile to be used for doing SAML SSO

appJson To store the template details in the json format.

Example

set vpn url wiurl -clientlessAccess on

show vpn url

Displays information about all the configured bookmark links to internal resources that appear in the Access Interface, or displays detailed information about the specified bookmark link.

Synopsis

show vpn url

Arguments

urlName Name of the bookmark link for which to display detailed information.

Output

linkName Description of the bookmark link. The description appears in the Access Interface.

vServerName Name of the associated LB/CS vserver

actualURL Web address for the bookmark link.

clientlessAccess Whether clientless access is enabled for the url in other modes or not.

comment Comments associated with this virtual server.

iconURL URL to fetch icon file for displaying this resource.

ssotype Single sign on type for unified gateway

applicationtype The type of application this VPN URL represents. Possible values are CVPN/ SaaS/VPN

samlSSOProfile Profile to be used for doing SAML SSO

appJson To store the template details in the json format.

devno count stateflag

unset vpn url

Use this command to remove vpn url settings.Refer to the set vpn url command for meanings of the arguments.

Synopsis

unset vpn url <urlName>

vpn-urlAction

The following operations can be performed on "vpn-urlAction":

unset| rename| set| add| rm| show|

unset vpn urlAction

Use this command to remove vpn urlAction settings.Refer to the set vpn urlAction command for meanings of the arguments.

Synopsis

unset vpn urlAction <name>

rename vpn urlAction

Renames the specified vpn urlAction.

Synopsis

rename vpn urlAction <name>@ <newName>@

Arguments

name Existing name of the vpn urlAction.

newName New name for the vpn urlAction. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vpnurl action" or 'my vpnurl action').

Example

rename vpn urlAction oldname newname

set vpn urlAction

Modifies the specified parameters of a bookmark link to a resource that appears in the Access Interface.

Synopsis

set vpn urlAction <name>

Arguments

name Name of the bookmark link.

linkName Description of the bookmark link. The description appears in the Access Interface.

actualURL Web address for the bookmark link.

vServerName Name of the associated vserver to handle selfAuth SSO

clientlessAccess If clientless access to the resource hosting the link is allowed, also use clientless access for the bookmarked web address in the Secure Client Access based session. Allows single sign-on and other HTTP processing on NetScaler Gateway for HTTPS resources.

Possible values: ON, OFF Default value: OFF

comment Any comments associated with the bookmark link.

iconURL URL to fetch icon file for displaying this resource.

ssotype Single sign on type for unified gateway

Possible values: unifiedgateway, selfauth, samlauth

applicationtype The type of application this VPN URL represents. Possible values are CVPN/ SaaS/VPN

Possible values: CVPN, VPN, SaaS

samlSSOProfile Profile to be used for doing SAML SSO

Example

set vpn urlAction wiurlaction -clientlessAccess on

add vpn urlAction

Creates a bookmark link to an external or internal resource that appears on the Access Interface, according to type, as a web site link or file share link.

Synopsis

add vpn urlAction <name> -linkName <string> -actualURL <string>

Arguments

name Name of the bookmark link.

linkName Description of the bookmark link. The description appears in the Access Interface.

actualURL Web address for the bookmark link.

vServerName Name of the associated vserver to handle selfAuth SSO

clientlessAccess If clientless access to the resource hosting the link is allowed, also use clientless access for the bookmarked web address in the Secure Client Access based session. Allows single sign-on and other HTTP processing on NetScaler Gateway for HTTPS resources.

Possible values: ON, OFF Default value: OFF

comment Any comments associated with the bookmark link.

iconURL URL to fetch icon file for displaying this resource.

ssotype Single sign on type for unified gateway

Possible values: unifiedgateway, selfauth, samlauth

applicationtype The type of application this VPN URL represents. Possible values are CVPN/ SaaS/VPN

Possible values: CVPN, VPN, SaaS

samlSSOProfile Profile to be used for doing SAML SSO

Example

add vpn urlAction ggl -linkName search -actualUrl www.google.com.

rm vpn urlAction

Removes a bookmark link to a resource that appears in the Access Interface.

Synopsis

rm vpn urlAction <name>

Arguments

name Name of the bookmark link.

Example

rm vpn urlAction ggl

show vpn urlAction

Displays information about all the configured bookmark links to resources that appear in the Access Interface, or displays detailed information about the specified bookmark link.

Synopsis

show vpn urlAction

Arguments

name Name of the bookmark link for which to display detailed information.

Output

linkName Description of the bookmark link. The description appears in the Access Interface.

vServerName Name of the associated vserver to handle selfAuth SSO

actualURL Web address for the bookmark link.

clientlessAccess If clientless access to the resource hosting the link is allowed, also use clientless access for the bookmarked web address in the Secure Client Access based session. Allows single sign-on and other HTTP processing on NetScaler Gateway for HTTPS resources.

comment Any comments associated with the bookmark link.

iconURL URL to fetch icon file for displaying this resource.

ssotype Single sign on type for unified gateway

applicationtype The type of application this VPN URL represents. Possible values are CVPN/ SaaS/VPN

samlSSOProfile Profile to be used for doing SAML SSO

devno count stateflag

vpn-urlPolicy

The following operations can be performed on "vpn-urlPolicy":

stat| add| set| rm| unset| rename| show|

stat vpn urlPolicy

Display vpn urlPolicy statistics.

Synopsis

stat vpn urlPolicy

Arguments

name The name of the vpn urlPolicy for which statistics will be displayed. If not given statistics are shown for all policies.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

Policy hits (Hits) Number of hits on the policy

Example

stat vpn urlPolicy

Related Commands

- stat vpn vserver

add vpn urlPolicy

Creates a new urlPolicy that, if bound, determines whether the URL is accessible or not.

Synopsis

add vpn urlPolicy <name> -rule <expression> -action <string>

Arguments

name Name for the new urlPolicy.

rule Expression, or name of a named expression, specifying the traffic that matches the policy.

The following requirements apply only to the NetScaler CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Action to be applied by the new urlPolicy if the rule criteria are met.

comment Any comments to preserve information about this policy.

logAction Name of messagelog action to use when a request matches this policy.

set vpn urlPolicy

Modifies the rule, action, comment and logAction of a urlPolicy.

Synopsis

set vpn urlPolicy <name>

Arguments

name Name for the new urlPolicy.

rule Expression, or name of a named expression, specifying the traffic that matches the policy.

The following requirements apply only to the NetScaler CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Action to be applied by the new urlPolicy if the rule criteria are met.

comment Any comments to preserve information about this policy.

logAction Name of messagelog action to use when a request matches this policy.

rm vpn urlPolicy

Removes the urlPolicy that is applied.

Synopsis

rm vpn urlPolicy <name>

Arguments

name Name for the new urlPolicy.

unset vpn urlPolicy

Use this command to remove vpn urlPolicy settings.Refer to the set vpn urlPolicy command for meanings of the arguments.

Synopsis

unset vpn urlPolicy <name>

rename vpn urlPolicy

Renames the specified vpn urlPolicy.

Synopsis

rename vpn urlPolicy <name>@ <newName>@

Arguments

name Existing name of the vpn urlPolicy.

newName New name for the vpn urlPolicy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vpnurl policy" or 'my vpnurl policy').

Example

rename vpn urlPolicy oldname newname

show vpn urlPolicy

Displays a urlPolicy.

Synopsis

show vpn urlPolicy

Arguments

name Name for the new urlPolicy.

Output

stateflag rule Expression, or name of a named expression, specifying the traffic that matches the policy.

The following requirements apply only to the NetScaler CLI:

- If the expression includes one or more spaces, enclose the entire expression in double quotation marks.
- If the expression itself includes double quotation marks, escape the quotations by using the \ character.
- Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

action Action to be applied by the new urlPolicy if the rule criteria are met.

comment Any comments to preserve information about this policy.

logAction Name of messagelog action to use when a request matches this policy.

boundTo The entity name to which policy is bound

activePolicy priority builtin Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

piHits Number of hits.

undefHits The number of times the policy evaluation resulted in undefined processing.

type Bindpoint to which the policy is bound

type Bindpoint to which the policy is bound

devno count

vpn-vserver

The following operations can be performed on "vpn-vserver":

disable| rename| rm| add| show| check| enable| unbind| stat| unset| set| bind|

disable vpn vserver

Disables a Citrix Gateway virtual server. The virtual server is taken out of service.

Synopsis

disable vpn vserver <name>@

Arguments

name Name of the virtual server to be disabled. The Citrix Gateway still responds to ARP and/or PING requests for the IP address of the virtual server. You can enable the Citrix Gateway virtual server again at any time, because the virtual server is still configured.

Example

disable vserver lb_vip

rename vpn vserver

Renames a Citrix Gateway virtual server.

Synopsis

rename vpn vserver <name>@ <newName>@

Arguments

name Name of the Citrix Gateway virtual server.

newName New name for the Citrix Gateway virtual server. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my server" or 'my server').

Example

rename vpn vserver vpn1 vpn1new

rm vpn vserver

Removes a Citrix Gateway virtual server. Policies that are bound to the virtual server are automatically unbound.

Synopsis

rm vpn vserver <name>@ ...

Arguments

name Name of the virtual server to remove.

Example

rm vserver vpn_vip

add vpn vserver

Creates a Citrix Gateway virtual server to allow authenticated users to access intranet resources, such as XenApp, XenDesktop, and web servers.

Synopsis

add vpn vserver <name> <serviceType> [<IPAddress>] [-Listenpolicy <expression>] [-maxLoginAttempts <positive_integer>]

Arguments

name Name for the Citrix Gateway virtual server. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the virtual server is created.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my server" or 'my server').

serviceType Protocol used by the Citrix Gateway virtual server.

Possible values: SSL, DTLS Default value: SSL

IPAddress IPv4 or IPv6 address of the Citrix Gateway virtual server. Usually a public IP address. User devices send connection requests to this IP address.

range Range of Citrix Gateway virtual server IP addresses. The consecutively numbered range of IP addresses begins with the address specified by the IP Address parameter. In the configuration utility, select Network VServer to enter a range. Default value: 1 Minimum value: 1

port TCP port on which the virtual server listens.

ipset The list of IPv4/IPv6 addresses bound to ipset would form a part of listening service on the current vpn vserver

state State of the virtual server. If the virtual server is disabled, requests are not processed.

Possible values: ENABLED, DISABLED Default value: ENABLED

authentication Require authentication for users connecting to Citrix Gateway.

Possible values: ON, OFF Default value: ON

doubleHop Use the Citrix Gateway appliance in a double-hop configuration. A double-hop deployment provides an extra layer of security for the internal network by using three firewalls to divide the DMZ into two stages. Such a deployment can have one appliance in the DMZ and one appliance in the secure network.

Possible values: ENABLED, DISABLED Default value: DISABLED

maxAAAUsers Maximum number of concurrent user sessions allowed on this virtual server. The actual number of users allowed to log on to this virtual server depends on the total number of user licenses. Minimum value: 0

icaOnly

- When set to ON, it implies Basic mode where the user can log on using either Citrix Receiver or a browser and get access to the published apps configured at the XenApp/XenDEsktop environment pointed out by the WIHome parameter. Users are not allowed to connect using the Citrix Gateway Plug-in and end point scans cannot be configured. Number of users that can log in and access the apps are not limited by the license in this mode.
- When set to OFF, it implies Smart Access mode where the user can log on using either Citrix Receiver or a browser or a Citrix Gateway Plug-in. The admin can configure end point scans to be run on the client systems and then use the results to control access to the published apps. In this mode, the client can connect to the gateway in other client modes namely VPN and CVPN. Number of users that can log in and access the resources are limited by the CCU licenses in this mode.

Possible values: ON, OFF Default value: OFF

icaProxySessionMigration This option determines if an existing ICA Proxy session is transferred when the user logs on from another device.

Possible values: ON, OFF Default value: OFF

dtls This option starts/stops the turn service on the vserver

Possible values: ON, OFF Default value: ON

loginOnce This option enables/disables seamless SSO for this Vserver.

Possible values: ON, OFF Default value: OFF

deviceCert Indicates whether device certificate check as a part of EPA is on or off.

Possible values: ON, OFF Default value: OFF

certkeyNames Name of the certificate key that was bound to the corresponding SSL virtual server as the Certificate Authority for the device certificate

downStateFlush Close existing connections when the virtual server is marked DOWN, which means the server might have timed out. Disconnecting existing connections frees resources and in certain cases speeds recovery of overloaded load balancing setups. Enable this setting on servers in which the connections can safely be closed when they are marked DOWN. Do not enable DOWN state flush on servers that must complete their transactions.

Possible values: ENABLED, DISABLED Default value: ENABLED

Listenpolicy String specifying the listen policy for the Citrix Gateway virtual server. Can be either a named expression or an expression. The Citrix Gateway virtual server processes only the traffic for which the expression evaluates to true. Default value: "none"

Listenpriority Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server, the virtual server whose listen policy has the highest priority (the lowest priority number) accepts the request. Default value: 101 Minimum value: 0 Maximum value: 100

tcpProfileName Name of the TCP profile to assign to this virtual server.

httpProfileName Name of the HTTP profile to assign to this virtual server. Default value: "nshttp_default_strict_validation"

comment Any comments associated with the virtual server.

appflowLog Log AppFlow records that contain standard NetFlow or IPFIX information, such as time stamps for the beginning and end of a flow, packet count, and byte count. Also log records that contain application-level information, such as HTTP web addresses, HTTP request methods and response status codes, server response time, and latency.

Possible values: ENABLED, DISABLED Default value: ENABLED

icmpVsrResponse Criterion for responding to PING requests sent to this virtual server. If this parameter is set to ACTIVE, respond only if the virtual server is available. With the PASSIVE setting, respond even if the virtual server is not available.

Possible values: PASSIVE, ACTIVE Default value: PASSIVE

RHIstate A host route is injected according to the setting on the virtual servers.

- If set to PASSIVE on all the virtual servers that share the IP address, the appliance always injects the hostroute.
- If set to ACTIVE on all the virtual servers that share the IP address, the appliance injects even if one virtual server is UP.
- If set to ACTIVE on some virtual servers and PASSIVE on the others, the appliance injects even if one virtual server set to ACTIVE is UP.

Possible values: PASSIVE, ACTIVE Default value: PASSIVE

netProfile The name of the network profile.

cginfraHomePageRedirect When client requests ShareFile resources and Citrix Gateway detects that the user is unauthenticated or the user session has expired, disabling this option takes the user to the originally requested ShareFile resource after authentication (instead of taking the user to the default VPN home page)

Possible values: ENABLED, DISABLED Default value: ENABLED

maxLoginAttempts Maximum number of logon attempts Minimum value: 1 Maximum value: 255

failedLoginTimeout Number of minutes an account will be locked if user exceeds maximum permissible attempts Minimum value: 1

l2Conn Use Layer 2 parameters (channel number, MAC address, and VLAN ID) in addition to the 4-tuple (<source IP>:<source port>::<destination IP>:<destination port>) that is used to identify a connection. Allows multiple TCP and non-TCP connections with the same 4-tuple to coexist on the Citrix ADC.

Possible values: ON, OFF

deploymentType rdpServerProfileName Name of the RDP server profile associated with the vserver.

WindowsEPAPluginUpgrade Option to set plugin upgrade behaviour for Win

Possible values: Always, Essential, Never

LinuxEPAPluginUpgrade Option to set plugin upgrade behaviour for Linux

Possible values: Always, Essential, Never

MacEPAPluginUpgrade Option to set plugin upgrade behaviour for Mac

Possible values: Always, Essential, Never

logoutOnSmartcardRemoval Option to VPN plugin behavior when smartcard or its reader is removed

Possible values: ON, OFF Default value: OFF

authnProfile Authentication Profile entity on virtual server. This entity can be used to offload authentication to AAA vserver for multi-factor(nFactor) authentication

vserverFqdn Fully qualified domain name for a VPN virtual server. This is used during StoreFront configuration generation.

pcoipVserverProfileName Name of the PCoIP vserver profile associated with the vserver.

SameSite SameSite attribute value for Cookies generated in VPN context. This attribute value will be appended only for the cookies which are specified in the builtin patset ns_cookies_samesite

Possible values: None, LAX, STRICT

Example

The following example creates a VPN virtual server named myvpnvip which supports SSL protocols and with AAA functionality enabled: vserver myvpnvip SSL 65.219.17.34 443 -aaa ON

show vpn vserver

Displays information about all the configured Citrix Gateway virtual servers, or displays detailed information about the specified Citrix Gateway virtual server.

Synopsis

show vpn vserver show vpn vserver stats - alias for 'stat vpn vserver'

Arguments

name Name of the Citrix Gateway virtual server for which to show detailed information.

Output

IPAddress The Virtual IP address of the VPN virtual server.

IPAddress The IP address of the virtual server.

value Indicates whether or not the certificate is bound or if SSL offload is disabled.

port The virtual TCP port of the VPN virtual server.

range The range of VPN virtual server IP addresses. The new range of VPN virtual servers will have IP addresses consecutively numbered, starting with the primary address specified with the <ipaddress> argument.

ipset The list of IPv4/IPv6 addresses bound to ipset would form a part of listening service on the current vpn vserver

serviceType The VPN virtual server's protocol type. Currently, the only possible value is SSL.

type The type of virtual server; for example, CONTENT based or ADDRESS based.

state The current state of the virtual server, as UP, DOWN, BUSY, and so on.

status Whether or not this virtual server responds to ARPs and whether or not round-robin selection is temporarily in effect.

cacheType Virtual server cache type. The options are: TRANSPARENT, REVERSE, and FORWARD.

redirect The cache redirect policy. The valid redirect policies are: l. CACHE - Directs all requests to the cache.

1. POLICY - Applies cache redirection policy to determine whether the request should be directed to the cache or origin. This is the default setting.
2. ORIGIN - Directs all requests to the origin server.

precedence This argument is used only when configuring content switching on the specified virtual server. This is applicable only if both the URL and RULE-based policies have been configured on the same virtual server. It specifies the type of policy (URL or RULE) that takes precedence on the content switching virtual server. The default setting is RULE. l URL - In this case, the incoming request is matched against the URL-based policies before the rule-based policies. l RULE - In this case, the incoming request is matched against the rule-based policies before the URL-based policies. For all URL-based policies, the precedence hierarchy is:

1. Domain and exact URL
2. Domain, prefix, and suffix
3. Domain and suffix
4. Domain and prefix
5. Domain only
6. Exact URL
7. Prefix and suffix
8. Suffix only
9. Prefix only
10. `Default`

redirectURL The URL where traffic is redirected if the virtual server in system becomes unavailable. WARNING! Make sure that the domain you specify in the URL does not match the domain specified in the -d domainName argument of the ###add cs policy### command. If the same domain is specified in both arguments, the request will be continuously redirected to the same unavailable virtual server in the system. If so, the user may not get the requested content.

authentication Indicates whether or not authentication is being applied to incoming users to the VPN.

doubleHop Indicates whether double-hop functionality is enabled or not.

icaOnly Indicates whether an ICA only license feature is enabled or not.

icaProxySessionMigration This option determines if an existing ICA Proxy session is transferred when the user logs on from another device.

dtls This option starts/stops Turn service on the vserver

loginOnce This option enables/disables seamless SSO for this Vserver.

advancedEpa Indicates whether advanced EPA feature is enabled or not.

deviceCert Indicates whether device certificate check as a part of EPA is enabled or not.

certkeyNames Name of the certificate key which was bound to the corresponding SSL virtual server as the Certificate Authority for the device certificate

maxAAAUsers The maximum number of concurrent users allowed to log on into this virtual server at a time.

curAAAUsers The number of current users logged on to this virtual server.

curTotalUsers The total number of current users connected through this virtual server.

domain The domain name of the server for which a service needs to be added. If the IP address has been specified, the domain name does not need to be specified.

rule The name of the rule, or expression, if any, that policy for the VPN server is to use. Rules are combinations of expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide. The default rule is true.

policyName The name of the policy, if any, bound to the VPN virtual server.

policy The name of the policy, if any, bound to the VPN virtual server.

serviceName The name of the service, if any, to which the virtual server policy is bound.

weight Weight for this service, if any. This weight is used when the system performs load balancing, giving greater priority to a specific service. It is useful when the services bound to a virtual server are of different capacity.

cacheVserver The name of the default target cache virtual server, if any, to which requests are redirected.

backupVServer The name of the backup VPN virtual server for this VPN virtual server.

priority Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000.

cltTimeout The idle time, if any, in seconds after which the client connection is terminated.

soMethod VPN client applications are allocated from a block of intranet IP addresses. That block may be exhausted after a certain number of connections. This switch specifies the method used to determine whether or not a new connection will spill over, or exhaust, the allocated block of intranet IP addresses for that application. Possible values are CONNECTION or DYNAMICCONNECTION. CONNECTION means that a static integer value is the hard limit for the spillover threshold. The

spillover threshold is described below. DYNAMICCONNECTION means that the spillover threshold is set according to the maximum number of connections defined for the VPN virtual server.

soThreshold VPN client applications are allocated from a block of intranet IP addresses. That block may be exhausted after a certain number of connections. The value of this option is the number of client connections after which the mapped IP address is used as the client source IP address instead of an address from the allocated block of intranet IP addresses.

soPersistence Whether or not cookie-based site persistance is enabled for this VPN vserver. Possible values are 'ConnectionProxy', HTTPRedirect, or NONE

soPersistenceTimeOut The timeout, if any, for cookie-based site persistance of this VPN vserver.

actType intranetApplication The intranet VPN application.

nextHopServer The name of the next hop server bound to the VPN virtual server.

urlName The intranet URL.

intranetIP The network ID for the range of intranet IP addresses or individual intranet IP addresses to be bound to the virtual server.

netmask The netmask of the intranet IP address or range.

intranetIP6 The network id for the range of intranet IP6 addresses or individual intranet ip to be bound to the vserver.

numaddr The number of ipv6 addresses

staServer Configured Secure Ticketing Authority (STA) server.

staAddressType Type of the STA server address(ipv4/v6).

staAuthID Authority ID of the STA Server. Authority ID is used to match incoming STA tickets in the SOCKS/CGP protocol with the right STA server.

staState State of the STA Server. If Authority ID is set then STA Server is UP else DOWN.

appController Configured App Controller server in XenMobile deployment.

sharefile Configured ShareFile server in XenMobile deployment. Format IP:PORT / FQDN:PORT

useMIP Deprecated. See 'map' below.

map Whether or not mapped IP addresses are ON or OFF. Mapped IP addresses are source IP addresses for the virtual servers running on the Citrix ADC. Mapped IP addresses are used by the system to connect to the backend servers.

downStateFlush Close existing connections when the virtual server is marked DOWN, which means the server might have timed out. Disconnecting existing connections frees resources and in certain cases speeds recovery of overloaded load balancing setups. Enable this setting on servers in which the connections can safely be closed when they are marked DOWN. Do not enable DOWN state flush on servers that must complete their transactions.

type Bindpoint to which the policy is bound.

gotoPriorityExpression Next priority expression.

disablePrimaryOnDown Tells whether traffic will continue reaching backup virtual servers even after the primary virtual server comes UP from DOWN state.

Listenpolicy The string is listenpolicy configured for VPN vserver

Listenpriority This parameter is the priority for listen policy of VPN Vserver.

tcpProfileName Name of the TCP profile to assign to this virtual server.

httpProfileName Name of the HTTP profile to assign to this virtual server.

policySubType stateflag flags comment Any comments associated with the virtual server.

appflowLog Log AppFlow records that contain standard NetFlow or IPFIX information, such as time stamps for the beginning and end of a flow, packet count, and byte count. Also log records that contain application-level information, such as HTTP web addresses, HTTP request methods and response status codes, server response time, and latency.

icmpVsrResponse Criterion for responding to PING requests sent to this virtual server. If this parameter is set to ACTIVE, respond only if the virtual server is available. With the PASSIVE setting, respond even if the virtual server is not available.

RHIstate A host route is injected according to the setting on the virtual servers.

- If set to PASSIVE on all the virtual servers that share the IP address, the appliance always injects the hostroute.
- If set to ACTIVE on all the virtual servers that share the IP address, the appliance injects even if one virtual server is UP.

- If set to ACTIVE on some virtual servers and PASSIVE on the others, the appliance injects even if one virtual server set to ACTIVE is UP.

netProfile The name of the network profile.

cginfraHomePageRedirect When client requests ShareFile resources and Citrix Gateway detects that the user is unauthenticated or the user session has expired, disabling this option takes the user to the originally requested ShareFile resource after authentication (instead of taking the user to the default VPN home page)

maxLoginAttempts Maximum number of logon attempts

failedLoginTimeout Number of minutes an account will be locked if user exceeds maximum permissible attempts

secondary Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.

groupExtraction Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.

deploymentType WindowsEPAPluginUpgrade Option to set plugin upgrade behaviour for Win

LinuxEPAPluginUpgrade Option to set plugin upgrade behaviour for Linux

MacEPAPluginUpgrade Option to set plugin upgrade behaviour for Mac

logoutOnSmartcardRemoval Option to VPN plugin behavior when smartcard or its reader is removed

epaprofile Advanced EPA profile to bind

epaprofileoptional Mark the EPA profile optional for preauthentication EPA profile. User would be shown a logon page even if the EPA profile fails to evaluate.

rdpServerProfileName Name of the RDP server profile associated with the vserver.

ngname Node group devno to which this authentication virtual sever belongs

state State of the virtual server. If the virtual server is disabled, requests are not processed.

vstype Virtual Server Type, such as Load Balancing, Content Switch, Cache Redirection

l2Conn Use Layer 2 parameters (channel number, MAC address, and VLAN ID) in addition to the 4-tuple (<source IP>:<source port>::<destination IP>:<destination port>) that is used to identify a connection. Allows multiple TCP and non-TCP connections with the same 4-tuple to coexist on the Citrix ADC.

portaltheme Name of the portal theme bound to VPN vserver

eula Name of the EULA bound to VPN vserver

userDomains List of user domains specified as comma seperated value

csVserver Name of the CS vserver to which the VPN vserver is bound

authnProfile Authentication Profile entity on virtual server. This entity can be used to offload authentication to AAA vserver for multi-factor(nFactor) authentication

vserverFqdn Fully qualified domain name for a VPN virtual server. This is used during StoreFront configuration generation.

pcoipVserverProfileName Name of the PCoIP vserver profile associated with the vserver.

analyticsProfile Name of the analytics profile bound to the VPN Vserver

noDefaultBindings to determine if the configuration will have default ssl CIPHER and ECC curve bindings

SameSite SameSite attribute value for Cookies generated in VPN context. This attribute value will be appended only for the cookies which are specified in the builtin patset ns_cookies_samesite

devno count

Example

show vpn vserver

check vpn vserver

Invokes Cerebro executable for connectivity checks for the servers bound to a VPN virtual server

Synopsis

check vpn vserver <name>

Arguments

name Name of the Citrix Gateway virtual server.

Output

response

Example

check vpn vserver <vserver name>

enable vpn vserver

Enables a Citrix Gateway virtual server. Note: Virtual servers, when added, are enabled by default.

Synopsis

enable vpn vserver <name>@

Arguments

name Name of the virtual server to be enabled.

Example

enable vserver vpn1

unbind vpn vserver

Unbinds the specified attributes from a virtual server.

Synopsis

unbind vpn vserver <name> [-policy <string>]

Arguments

name Name of the virtual server from which to unbind an attribute.

policy Name of the policy to unbind from the virtual server.

secondary Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.

groupExtraction Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.

type Bind point from which to unbind the policy.

Possible values: REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE

intranetApplication Name of intranet application to unbind from the virtual server.

nextHopServer Name of the next hop server to remove.

urlName Web address of the next hop virtual server to unbind.

intranetIP The range of IP addresses to unbind from the virtual server.

netmask The netmask of the intranet IP address or range.

intranetIP6 The range of IP addresses to unbind from the virtual server.

numaddr The number of ipv6 addresses Minimum value: 1

staServer Web address of the Secure Ticket Authority (STA) server to remove, in the following format: 'http(s)://FQDN/URLPATH'

appController App Controller server to be removed, in the format 'http(s)://IP/FQDN'

sharefile ShareFile server to be removed, in the format 'IP:PORT / FQDN:PORT'

portaltheme Name of the Portal theme to unbind from vpn vserver

eula Name of EULA to unbind from vpn vserver

analyticsProfile unbind lb vserver <vserver_name> -analyticsProfile <analytics-profile-name>.

stat vpn vserver

Displays statistics for all Citrix Gateway virtual servers, or displays detailed statistics for the specified Citrix Gateway virtual server.

Synopsis

stat vpn vserver

Arguments

name Name of the virtual server for which to show detailed statistics.

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

count devno stateflag

Counters

IP address (IP) The IP address on which the service is running.

Port (port) The port on which the service is running.

Vserver protocol (Protocol) Protocol associated with the vserver

State Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)

Requests (Req) Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Responses (Rsp) Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

Request bytes (Reqb) Total number of request bytes received on this service or virtual server.

Response bytes (Rspb) Number of response bytes received by this service or virtual server.

Current Users (curusers) Number of users on this vserver

Current AAA Sessions (cursess) Number of aaa sessions on this vserver

Related Commands

- stat vpn urlPolicy

unset vpn vserver

Use this command to remove vpn vserver settings.Refer to the set vpn vserver command for meanings of the arguments.

Synopsis

unset vpn vserver <name>

set vpn vserver

Modifies the specified parameters of a Citrix Gateway virtual server.

Synopsis

set vpn vserver <name>

Arguments

name Name of the virtual server to modify.

IPAddress IPv4 or IPv6 address of the Citrix Gateway virtual server. Usually a public IP address. User devices send connection requests to this IP address.

ipset The list of IPv4/IPv6 addresses bound to ipset would form a part of listening service on the current vpn vserver

authentication Require authentication for users connecting to Citrix Gateway.

Possible values: ON, OFF Default value: ON

doubleHop Use the Citrix Gateway appliance in a double-hop configuration. A double-hop deployment provides an extra layer of security for the internal network by using three firewalls to divide the DMZ into two stages. Such a deployment can have one appliance in the DMZ and one appliance in the secure network.

Possible values: ENABLED, DISABLED Default value: DISABLED

icaOnly

- When set to ON, it implies Basic mode where the user can log on using either Citrix Receiver or a browser and get access to the published apps configured at the XenApp/XenDEsktop environment pointed out by the WIHome parameter. Users are not allowed to connect using the Citrix Gateway Plug-in and end point scans cannot be configured. Number of users that can log in and access the apps are not limited by the license in this mode.
- When set to OFF, it implies Smart Access mode where the user can log on using either Citrix Receiver or a browser or a Citrix Gateway Plug-in. The admin can configure end point scans to be run on the client systems and then use the results to control access to the published apps. In this mode, the client can connect to the gateway in other client modes namely VPN and CVPN. Number of users that can log in and access the resources are limited by the CCU licenses in this mode.

Possible values: ON, OFF Default value: OFF

icaProxySessionMigration This option determines if an existing ICA Proxy session is transferred when the user logs on from another device.

Possible values: ON, OFF Default value: OFF

dtls This option starts/stops the turn service on the vserver

Possible values: ON, OFF Default value: ON

loginOnce This option enables/disables seamless SSO for this Vserver.

Possible values: ON, OFF Default value: OFF

deviceCert Indicates whether device certificate check as a part of EPA is enabled or not.

Possible values: ON, OFF Default value: OFF

certkeyNames Name of the certkey which was bound to the corresponding SSL virtual server as the Certificate Authority for the device certificate

maxAAAUsers Maximum number of concurrent user sessions allowed on this virtual server. The actual number of users allowed to log on to this virtual server depends on the total number of user licenses. Minimum value: 0

downStateFlush Close existing connections when the virtual server is marked DOWN, which means the server might have timed out. Disconnecting existing connections frees resources and in certain cases speeds recovery of overloaded load balancing setups. Enable this setting on servers

in which the connections can safely be closed when they are marked DOWN. Do not enable DOWN state flush on servers that must complete their transactions.

Possible values: ENABLED, DISABLED Default value: ENABLED

Listenpolicy String specifying the listen policy for the Citrix Gateway virtual server. Can be either a named expression or an expression. The Citrix Gateway virtual server processes only the traffic for which the expression evaluates to true. Default value: "none"

Listenpriority Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server, the virtual server whose listen policy has the highest priority (the lowest priority number) accepts the request. Default value: 101 Minimum value: 0 Maximum value: 100

tcpProfileName Name of the TCP profile to assign to this virtual server.

httpProfileName Name of the HTTP profile to assign to this virtual server. Default value: "nshttp_default_strict_validation"

comment Any comments associated with the virtual server.

appflowLog Log AppFlow records that contain standard NetFlow or IPFIX information, such as time stamps for the beginning and end of a flow, packet count, and byte count. Also log records that contain application-level information, such as HTTP web addresses, HTTP request methods and response status codes, server response time, and latency.

Possible values: ENABLED, DISABLED Default value: ENABLED

icmpVsrResponse Criterion for responding to PING requests sent to this virtual server. If this parameter is set to ACTIVE, respond only if the virtual server is available. With the PASSIVE setting, respond even if the virtual server is not available.

Possible values: PASSIVE, ACTIVE Default value: PASSIVE

RHIstate A host route is injected according to the setting on the virtual servers.

- If set to PASSIVE on all the virtual servers that share the IP address, the appliance always injects the hostroute.
- If set to ACTIVE on all the virtual servers that share the IP address, the appliance injects even if one virtual server is UP.
- If set to ACTIVE on some virtual servers and PASSIVE on the others, the appliance injects even if one virtual server set to ACTIVE is UP.

Possible values: PASSIVE, ACTIVE Default value: PASSIVE

netProfile The name of the network profile.

cginfraHomePageRedirect When client requests ShareFile resources and Citrix Gateway detects that the user is unauthenticated or the user session has expired, disabling this option takes the user to the originally requested ShareFile resource after authentication (instead of taking the user to the default VPN home page)

Possible values: ENABLED, DISABLED Default value: ENABLED

maxLoginAttempts Maximum number of logon attempts Minimum value: 1 Maximum value: 255

rdpServerProfileName Name of the RDP server profile associated with the vserver.

failedLoginTimeout Number of minutes an account will be locked if user exceeds maximum permissible attempts Minimum value: 1

l2Conn Use Layer 2 parameters (channel number, MAC address, and VLAN ID) in addition to the 4-tuple (<source IP>:<source port>::<destination IP>:<destination port>) that is used to identify a connection. Allows multiple TCP and non-TCP connections with the same 4-tuple to coexist on the Citrix ADC.

Possible values: ON, OFF

WindowsEPAPluginUpgrade Option to set plugin upgrade behaviour for Win

Possible values: Always, Essential, Never

MacEPAPluginUpgrade Option to set plugin upgrade behaviour for Mac

Possible values: Always, Essential, Never

LinuxEPAPluginUpgrade Option to set plugin upgrade behaviour for Linux

Possible values: Always, Essential, Never

logoutOnSmartcardRemoval Option to VPN plugin behavior when smartcard or its reader is removed

Possible values: ON, OFF Default value: OFF

authnProfile Authentication Profile entity on virtual server. This entity can be used to offload authentication to AAA vserver for multi-factor(nFactor) authentication

vserverFqdn Fully qualified domain name for a VPN virtual server. This is used during StoreFront configuration generation.

pcoipVserverProfileName Name of the PCoIP vserver profile associated with the vserver.

SameSite SameSite attribute value for Cookies generated in VPN context. This attribute value will be appended only for the cookies which are specified in the builtin patset ns_cookies_samesite

Possible values: None, LAX, STRICT

bind vpn vserver

Binds attributes to the specified Citrix Gateway virtual server.

Synopsis

bind vpn vserver <name> [-policy <string>] [-staServer <URL>]

Arguments

name Name of the virtual server.

policy Name of a policy to bind to the virtual server (for example, the name of an authentication, session, or endpoint analysis policy).

priority Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value: 0 Maximum value: 2147483647

secondary Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.

groupExtraction Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.

gotoPriorityExpression Applicable only to advance vpn session policy. Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values:

- NEXT - Evaluate the policy with the next higher priority number.
- END - End policy evaluation.
- An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows:
- If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next.
- If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next.
- If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if:
- The expression is invalid.
- The expression evaluates to a priority number that is numerically lower than the current policy's priority.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

type Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression.

Possible values: REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE

intranetApplication Name of the application to bind to the virtual server. Intranet applications are used to enable access to selected applications located in the internal network. They are required for any user connecting with the Citrix Gateway Plug-in for Java.

nextHopServer Name of the next hop server to bind to the virtual server.

urlName Web address of the next hop virtual server to bind to the virtual server.

intranetIP The network ID for the range of intranet IP addresses or individual intranet IP addresses to be bound to the virtual server.

netmask A range of IP addresses in an address pool, bound to a virtual server. When users log on, Citrix Gateway assigns an IP address from the pool.

intranetIP6 The network id for the range of intranet IP6 addresses or individual intranet ip to be bound to the vserver.

numaddr A range of IP addresses in an address pool, bound to a virtual server. When users log on, Access Gateway assigns an IP address from the pool. Minimum value: 1

staServer Web address of the Secure Ticket Authority (STA) server, in the following format: 'http(s)://FQDN/URLPATH'

staAddressType Type of the STA server address(ipv4/v6).

Possible values: IPV4, IPV6

appController App Controller server, in the format 'http(s)://IP/FQDN'

sharefile ShareFile server, in the format 'IP:PORT / FQDN:PORT'

portaltheme Name of Portal theme to bind to vpn vserver

eula Name of EULA to bind to vpn vserver

analyticsProfile bind lb vserver <vserver_name> -analyticsProfile <analytics-profile-name>.

vpn

The following operations can be performed on "vpn":

stat vpn

Displays the statistics for Citrix Gateway usage. Displays event information, such as the event that generated the message, a time stamp, the message type, and predefined log levels and message information.

Synopsis

stat vpn

Arguments

detail Specifies detailed output (including more statistics). The output can be quite voluminous. Without this argument, the output will show only a summary.

fullValues Specifies that numbers and strings should be displayed in their full form. Without this option, long strings are shortened and large numbers are abbreviated

ntimes The number of times, in intervals of seven seconds, the statistics should be displayed. Default value: 1 Minimum value: 0

logFile The name of the log file to be used as input.

clearstats Clear the statsistics / counters

Possible values: basic, full

Output

Counters

Login-page requests received (iHtHit) Number of requests for VPN login page.

Login-page delivery failures (iHtFail) Number of failures to display VPN login page.

Client-configuration requests (cfgHit) Number of client configuration requests received by VPN server.

DNS queries resolved (dnsHit) Number of DNS queries resolved by VPN server.

WINS queries resolved (winsHit) Number of WINS queries resolved by VPN server.

Number of SSLVPN tunnels (csHit) Number of SSL VPN tunnels formed between VPN server and client.

Backend non-HTTP server probes (csNoHttp) Number of probes from VPN to back-end non-HTTP servers that have been accessed by the VPN client.

Backend HTTP server probes (csHttp) Number of probes from VPN to back-end HTTP servers that have been accessed by the VPN client.

Backend server probe successes (csConSuc) Number of successful probes to all back-end servers.

File-system requests received (totFsHit) Number of file system requests received by VPN server.

VPN User License Not Available (licFail) Number of users not able to login because of license unavailability.

Requests from VPN to Apache (svpnhttpdTotalReq) Total number of requests from VPN to Apache

Responses from Apache for VPN (svpnhttpdTotalResp) Total number of responses from Apache for VPN

Requests to Apache cache hits (svpnhttpdTotalReqCacheHits) Total number of vpn requests to Apache hitting cache

VPN to Apache open connections (svpnhttpdCurServerConnections) Number of current VPN to Apache open server connections

IIP disabled and SNIP used (IIPdMIPu) Number of times SNIP is used as IIP is disabled.

IIP failed and SNIP used (IIPfMIPu) Number of times SNIP is used as IIP assignment failed.

IIP spillover and SNIP used (IIPsMIPu) Number of times SNIP is used on IIP Spillover.

IIP disabled and SNIP disabled (IIPdMIPd) Both IIP and SNIP is disabled.

IIP failed and SNIP disabled (IIPfMIPd) Number of times IIP assignment failed and SNIP is disabled.

Current users across vservers (CsgTotalConnectedUsers) Number of total users connected across VPN vservers

SOCKS method request received (SOCKSmReqR) Number of received SOCKS method request.

SOCKS method request sent (SOCKSmReqS) Number of sent SOCKS method request.

SOCKS method response received (SOCKSmRespR) Number of received SOCKS method response.

SOCKS method response sent (SOCKSmRespS) Number of sent SOCKS method response.

SOCKS connect request received (SOCKScReqR) Number of received SOCKS connect request.

SOCKS connect request sent (SOCKScReqS) Number of sent SOCKS connect request.

SOCKS connect response received (SOCKScRespR) Number of received SOCKS connect response.

SOCKS connect response sent (SOCKScRespS) Number of sent SOCKS connect response.

SOCKS server error (SOCKSserverErr) Number of SOCKS server error.

SOCKS client error (SOCKSclientErr) Number of SOCKS client error.

STA connection success (STAconnSucc) Number of STA connection success.

STA connection failure (STAconnFail) Number of STA connection failure.

CPS connection success (CPSconnSucc) Number of CPS connection success.

CPS connection failure (CPSconnFail) Number of CPS connection failure.

STA request sent (STAreqSent) Number of STA request sent.

STA response received (STArespRecvd) Number of STA response received.

ICA license failure (ICAlicenseFail) Number of ICA license failure.

STA monitor requests sent (STAmonSent) Number of STA monitor requests sent.

STA monitor reponses recieved (STAmonRcvd) Number of STA monitor responses recieved.

STA monitor successful responses (STAmonSucc) Number of STA monitor successful responses.

STA monitor failed responses (STAmonFail) Number of STA monitor failed responses.

Primary STA lookup failed (CsgPtktValidateNotStarted) Total number of STA server lookup failures for auth-id in primary ticket

Redundant STA lookup failed (CsgRtktValidateNotStarted) Total number of STA server lookup failures for auth-id in redundant ticket

Related Commands

- stat vpn urlPolicy