Citrix ADC SNMP OID Reference

A detailed list of the SNMP OIDs that can be used to obtain information from a Citrix ADC appliance.

- Generic MIB-II OIDs
- lldpConfiguration
- lldpStatistics
- lldpStatsTxPortTable
- lldpStatsRxPortTable
- lldpLocalSystemData
- lldpLocPortTable
- lldpLocManAddrTable
- lldpRemTable
- lldpRemManAddrTable
- system
- interfaces
- ifTable
- icmp
- udp
- udpTable
- snmp
- ifMIBObjects
- ifXTable
- Citrix ADC Enterprise OIDs
    - nsSysGroup
        - nsFeatureInfo
        - nsModeInfo

- aclStatsGroup
  - nsAclTable
- saclStatsGroup
- acl6StatsGroup
  - nsAcl6Table
- pbrStatsGroup
- nsPbrTable
- sacl6StatsGroup
- pbr6StatsGroup
  - nsPbr6Table
- nsHighAvailabilityGroup
- vlanTable
- nsIpAddrTable
- nsResourceGroup
  - nsCPUTable
  - nsSysHealthTable
  - nsSysHealthDiskTable
- nsIpStatsGroup
- nsIcmpStatsGroup
- nsUdpStatsGroup
- nsTcpStatsGroup
- nsSslStatsGroup
- nsHttpStatsGroup
- nsCacheStatsGroup
- nsCompressionStatsGroup
- gslbGlobalStats
- gslbSitesTable
- nsDomainTable

- nsPolicyStatsTable
- nsDnsServerStatsGroup
- nsdnsRegisterTable
- nsIfStatsTable
- scPolicyStatistics
- scPolicyConfigTable
- sslCertKeyTable
- sslCrlTable
- sslCipherGroupTable
- dosPolicyTable
- dosPolicyStatistics
- nsExpressionTable
- pqPolicyConfigTable
- pqPolicyStatistics
- crPolicyMapConfigTable
- appFirewallStatistics
- appfwProfileTable
- nsRnatGlobalStats
- nsRnatPerIPStatsTable
- nsSslVpnStatsGroup
- nsAaaStatsGroup
- nsGlobalConfigSettings
- piPolicyTable
- nsInetAddressTable
- nsNicStatsGroup
- clusterTable
- nsClusterStatsGroup
- nsInatGlobalStats
- nsInatPerNat46StatsTable
- nsInatPerNatStatsTable

- nsInatSessionGlobalStats
- nsNat64GlobalStats
- nsIp6StatsGroup
- nsTdInetAddressTable
- nsLLDPConfigGroup
- nsLLDPStatsGroup
  - nsLLDPStatsTxPortTable
  - nsLLDPStatsRxPortTable
- nsLLDPLocSystemsGroup
  - nsLLDPLocPortTable
  - nsLLDPLocManAddrTable
- nsLLDPRemTable
- nsLLDPRemManAddrTable
- vxlanTable
- cacheGroupTable
- nsLsnGlobalStatsGroup
- nsLsnGroupTable
- nsPPTPStatsGroup
- nsLsnDSLiteGlobalStatsGroup
- nsLsnLogStatsGroup
  - nsLsnMappingLogStatsGroup
  - nsLsnSessionLogStatsGroup
- nsLsnNAT64GlobalStatsGroup
- nsLsnPoolTable
- nsmcStatsGroup
- nsMapDomainStatsTable
- nsIpSecAlgProfTable
- nsRnat6GlobalStats

    - partitionTable
- botManagementStatistics
- botProfileTable
- nsHttp2StatsGroup
- icapStatistics
- inlineStatistics
- mirrorStatistics
- nsQuicStatsGroup
- nsQuicBridgeStatsGroup
- nsHttp3StatsGroup
- apiSpecTable
- apiEndpointTable
- serviceTable
- serverTable
- serviceScpolicyTable
- serviceAdvanceSslConfigTable
- serviceCipherBindingTable
- serviceGlobalStatsGroup
- serviceGroupMemberTable
- serviceDospolicyTable
- monitorMemberTable
- monServiceMemberTable
- serviceGroupTable
- vserverTable
- vserverServiceTable
- vserverCspolicyTable
- vserverCrpolicyTable
- (

#vserverglobalstatsgroup)

- lbvserverTable
- vserverPqpolicyTable
- vserverScpolicyTable
- vserverAdvanceSslConfigTable
- vserverCipherBindingTable
- vserverCsPiPolicyTable
- snmpTrapVarBindOidsGroup
- Generic MIB-II Traps
- Citrix ADC Enterprise Traps

Generic MIB-II OIDs

‹ Citrix ADC SNMP OID Reference

Generic MIB-II OIDs

lldpConfiguration

OID: 1.0.8802.1.1.2.1.1

lldpMessageTxInterval

OID:1.0.8802.1.1.2.1.1.1

The interval at which LLDP frames are transmitted on behalf of this LLDP agent. The default value for lldpMessageTxInterval object is 30 seconds. The value of this object must be restored from non-volatile storage after a re-initialization of the management system. REFERENCE IEEE 802.1AB-2005 10.5.3.3 DEFVAL { 30 }

lldpMessageTxHoldMultiplier

OID:1.0.8802.1.1.2.1.1.2

The time-to-live value expressed as a multiple of the lldpMessageTxInterval object. The actual time-to-live value used in LLDP frames, transmitted on behalf of this LLDP agent, can be expressed by the following formula: TTL = min(65535, (lldpMessageTxInterval * lldpMessageTxHoldMultiplier)) For example, if the value of lldpMessageTxInterval is '30', and the value of lldpMessageTxHoldMultiplier is '4', then the value '120' is encoded in the TTL field in the LLDP header. The default value for lldpMessageTxHoldMultiplier object is 4. The value of this object must be restored from non-volatile storage after a re-initialization of the management system. REFERENCE IEEE 802.1AB-2005 10.5.3.3 DEFVAL { 4 }

lldpReinitDelay

OID:1.0.8802.1.1.2.1.1.3

The lldpReinitDelay indicates the delay (in units of seconds) from when lldpPortConfigAdminStatus object of a particular port becomes 'disabled' until re-initialization will be attempted. The default value for lldpReintDelay object is two seconds. The value of this object must be restored from non-volatile storage after a re-initialization of the management system. REFERENCE IEEE 802.1AB-2005 10.5.3.3 DEFVAL { 2 }

lldpTxDelay

OID:1.0.8802.1.1.2.1.1.4

The lldpTxDelay indicates the delay (in units of seconds) between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB. The recommended value for the lldpTxDelay is set by the following formula: 1 <= lldpTxDelay <= (0.25 * lldpMessageTxInterval) The default value for lldpTxDelay object is two seconds. The value of this object must be restored from non-volatile storage after a re-initialization of the management system. REFERENCE IEEE 802.1AB-2005 10.5.3.3 DEFVAL { 2 }

lldpNotificationInterval

OID:1.0.8802.1.1.2.1.1.5

This object controls the transmission of LLDP notifications. the agent must not generate more than one lldpRemTablesChange notification-event in the indicated period, where a 'notification-event' is the transmission of a single notification PDU type to a list of notification destinations. If additional changes in lldpRemoteSystemsData object groups occur within the indicated throttling period, then these trap- events must be suppressed by the agent. An NMS should periodically check the value of lldpStatsRemTableLastChangeTime to detect any missed lldpRemTablesChange notification-events, e.g. due to throttling or transmission loss. If notification transmission is enabled for particular ports, the suggested default throttling period is 5 seconds. The value of this object must be restored from non-volatile storage after a re-initialization of the management system. DEFVAL { 5 }

lldpStatistics

OID: 1.0.8802.1.1.2.1.2

lldpStatsRemTablesLastChangeTime

OID:1.0.8802.1.1.2.1.2.1

The value of sysUpTime object (defined in IETF RFC 3418) at the time an entry is created, modified, or deleted in the in tables associated with the lldpRemoteSystemsData objects and all LLDP extension objects associated with remote systems. An NMS can use this object to reduce polling of the lldpRemoteSystemsData objects.

lldpStatsRemTablesInserts

OID:1.0.8802.1.1.2.1.2.2

The number of times the complete set of information advertised by a particular MSAP has been inserted into tables contained in lldpRemoteSystemsData and lldpExtensions objects. The complete set of information received from a particular MSAP should be inserted into related tables. If partial information cannot be inserted for a reason such as lack of resources, all of the complete set of information should be removed. This counter should be incremented only once after the complete set of information is successfully recorded in all related tables. Any failures during inserting information set which result in deletion of previously inserted information should not trigger any changes in lldpStatsRemTablesInserts since the insert is not completed yet or or in lldpStatsRemTablesDeletes, since the deletion would only be a partial deletion. If the failure was the result of lack of resources, the lldpStatsRemTablesDrops counter should be incremented once.

lldpStatsRemTablesDeletes

OID:1.0.8802.1.1.2.1.2.3

The number of times the complete set of information advertised by a particular MSAP has been deleted from tables contained in lldpRemoteSystemsData and lldpExtensions objects. This counter should be incremented only once when the complete set of information is completely deleted from all related tables. Partial deletions, such as deletion of rows associated with a particular MSAP from some tables, but not from all tables are not allowed, thus should not change the value of this counter.

lldpStatsRemTablesDrops

OID:1.0.8802.1.1.2.1.2.4

The number of times the complete set of information advertised by a particular MSAP could not be entered into tables contained in lldpRemoteSystemsData and lldpExtensions objects because of insufficient resources.

lldpStatsRemTablesAgeouts

OID:1.0.8802.1.1.2.1.2.5

The number of times the complete set of information advertised by a particular MSAP has been deleted from tables contained in lldpRemoteSystemsData and lldpExtensions objects because the information timeliness interval has expired. This counter should be incremented only once when the complete set of information is completely invalidated (aged out) from all related tables. Partial aging, similar to deletion case, is not allowed, and thus, should not change the value of this counter.

lldpStatsTxPortTable

OID: 1.0.8802.1.1.2.1.2.6

lldpStatsTxPortNum

OID:1.0.8802.1.1.2.1.2.6.1.1

The index value used to identify the port component (contained in the local chassis with the LLDP agent) associated with this entry. The value of this object is used as a port index to the lldpStatsTable.

lldpStatsTxPortFramesTotal

OID:1.0.8802.1.1.2.1.2.6.1.2

The number of LLDP frames transmitted by this LLDP agent on the indicated port. REFERENCE IEEE 802.1AB-2005 10.5.2.1

lldpStatsRxPortTable

OID: 1.0.8802.1.1.2.1.2.7

lldpStatsRxPortNum

OID:1.0.8802.1.1.2.1.2.7.1.1

The index value used to identify the port component (contained in the local chassis with the LLDP agent) associated with this entry. The value of this object is used as a port index to the lldpStatsTable.

lldpStatsRxPortFramesDiscardedTotal

OID:1.0.8802.1.1.2.1.2.7.1.2

The number of LLDP frames received by this LLDP agent on the indicated port, and then discarded for any reason. This counter can provide an indication that LLDP header formating problems may exist with the local LLDP agent in the sending system or that LLDPDU validation problems may exist with the local LLDP agent in the receiving system. REFERENCE IEEE 802.1AB-2005 10.5.2.2

lldpStatsRxPortFramesErrors

OID:1.0.8802.1.1.2.1.2.7.1.3

The number of invalid LLDP frames received by this LLDP agent on the indicated port, while this LLDP agent is enabled. REFERENCE IEEE 802.1AB-2005 10.5.2.2

lldpStatsRxPortFramesTotal

OID:1.0.8802.1.1.2.1.2.7.1.4

The number of valid LLDP frames received by this LLDP agent on the indicated port, while this LLDP agent is enabled. REFERENCE IEEE 802.1AB-2005 10.5.2.2

lldpStatsRxPortTLVsDiscardedTotal

OID:1.0.8802.1.1.2.1.2.7.1.5

The number of LLDP TLVs discarded for any reason by this LLDP agent on the indicated port. REFERENCE IEEE 802.1AB-2005 10.5.2.2

lldpStatsRxPortTLVsUnrecognizedTotal

OID:1.0.8802.1.1.2.1.2.7.1.6

The number of LLDP TLVs received on the given port that are not recognized by this LLDP agent on the indicated port. An unrecognized TLV is referred to as the TLV whose type value is in the range of reserved TLV types (000 1001 - 111 1110) in Table 9.1 of IEEE Std 802.1AB-2005. An unrecognized TLV may be a basic management TLV from a later LLDP version. REFERENCE IEEE 802.1AB-2005 10.5.2.2

lldpStatsRxPortAgeoutsTotal

OID:1.0.8802.1.1.2.1.2.7.1.7

The counter that represents the number of age-outs that occurred on a given port. An age-out is the number of times the complete set of information advertised by a particular MSAP has been

deleted from tables contained in lldpRemoteSystemsData and lldpExtensions objects because the information timeliness interval has expired. This counter is similar to lldpStatsRemTablesAgeouts, except that the counter is on a per port basis. This enables NMS to poll tables associated with the lldpRemoteSystemsData objects and all LLDP extension objects associated with remote systems on the indicated port only. This counter should be set to zero during agent initialization and its value should not be saved in non-volatile storage. When a port's admin status changes from 'disabled' to 'rxOnly', 'txOnly' or 'txAndRx', the counter associated with the same port should reset to 0. The agent should also flush all remote system information associated with the same port. This counter should be incremented only once when the complete set of information is invalidated (aged out) from all related tables on a particular port. Partial aging is not allowed, and thus, should not change the value of this counter. REFERENCE IEEE 802.1AB-2005 10.5.2.2

lldpLocalSystemData

OID: 1.0.8802.1.1.2.1.3

lldpLocChassisIdSubtype

OID:1.0.8802.1.1.2.1.3.1

The type of encoding used to identify the chassis associated with the local system. REFERENCE IEEE 802.1AB-2005 9.5.2.2

lldpLocChassisId

OID:1.0.8802.1.1.2.1.3.2

The type of encoding used to identify the chassis associated with the local system. REFERENCE IEEE 802.1AB-2005 9.5.2.2

lldpLocSysName

OID:1.0.8802.1.1.2.1.3.3

The string value used to identify the system name of the local system. If the local agent supports IETF RFC 3418, lldpLocSysName object should have the same value of sysName object. REFERENCE IEEE 802.1AB-2005 9.5.6.2

lldpLocSysDesc

OID:1.0.8802.1.1.2.1.3.4

The string value used to identify the system description of the local system. If the local agent supports IETF RFC 3418, lldpLocSysDesc object should have the same value of sysDesc object. REFERENCE IEEE 802.1AB-2005 9.5.7.2

lldpLocSysCapSupported

OID:1.0.8802.1.1.2.1.3.5

The bitmap value used to identify which system capabilities are supported on the local system. REFERENCE IEEE 802.1AB-2005 9.5.8.1

lldpLocSysCapEnabled

OID:1.0.8802.1.1.2.1.3.6

The bitmap value used to identify which system capabilities are enabled on the local system. REFERENCE IEEE 802.1AB-2005 9.5.8.2

lldpLocPortTable

OID: 1.0.8802.1.1.2.1.3.7

lldpLocPortNum

OID:1.0.8802.1.1.2.1.3.7.1.1

The index value used to identify the port component (contained in the local chassis with the LLDP agent) associated with this entry. The value of this object is used as a port index to the lldpLocPortTable.

lldpLocPortIdSubtype

OID:1.0.8802.1.1.2.1.3.7.1.2

The type of port identifier encoding used in the associated 'lldpLocPortId' object. REFERENCE IEEE 802.1AB-2005 9.5.3.2

lldpLocPortId

OID:1.0.8802.1.1.2.1.3.7.1.3

The type of port identifier encoding used in the associated 'lldpLocPortId' object. REFERENCE IEEE 802.1AB-2005 9.5.3.2

lldpLocPortDesc

OID:1.0.8802.1.1.2.1.3.7.1.4

The string value used to identify the 802 LAN station's port description associated with the local system. If the local agent supports IETF RFC 2863, lldpLocPortDesc object should have the same value of ifDescr object. REFERENCE IEEE 802.1AB-2005 9.5.5.2

lldpLocManAddrTable

OID: 1.0.8802.1.1.2.1.3.8

lldpLocManAddrSubtype

OID:1.0.8802.1.1.2.1.3.8.1.1

The type of management address identifier encoding used in the associated 'lldpLocManagmentAddr' object. REFERENCE IEEE 802.1AB-2005 9.5.9.3

lldpLocManAddr

OID:1.0.8802.1.1.2.1.3.8.1.2

This table contains management address information on the local system known to this agent.

lldpLocManAddrLen

OID:1.0.8802.1.1.2.1.3.8.1.3

The total length of the management address subtype and the management address fields in LLDPDUs transmitted by the local LLDP agent. The management address length field is needed so that the receiving systems that do not implement SNMP will not be required to implement an iana family numbers/address length equivalency table in order to decode the management adress. REFERENCE IEEE 802.1AB-2005 9.5.9.2

lldpLocManAddrIfSubtype

OID:1.0.8802.1.1.2.1.3.8.1.4

The enumeration value that identifies the interface numbering method used for defining the interface number, associated with the local system. REFERENCE IEEE 802.1AB-2005 9.5.9.5

lldpLocManAddrIfId

OID:1.0.8802.1.1.2.1.3.8.1.5

The integer value used to identify the interface number regarding the management address component associated with the local system. REFERENCE IEEE 802.1AB-2005 9.5.9.6

lldpLocManAddrOID

OID:1.0.8802.1.1.2.1.3.8.1.6

The OID value used to identify the type of hardware component or protocol entity associated with the management address advertised by the local system agent. REFERENCE IEEE 802.1AB-2005 9.5.9.8

lldpRemTable

OID: 1.0.8802.1.1.2.1.4.1

lldpRemTimeMark

OID:1.0.8802.1.1.2.1.4.1.1.1

A TimeFilter for this entry. See the TimeFilter textual convention in IETF RFC 2021 and http://www.ietf.org/IESG/Implementations/RFC2021-Implementation.txt to see how TimeFilter works. REFERENCE IETF RFC 2021 section 6

lldpRemLocalPortNum

OID:1.0.8802.1.1.2.1.4.1.1.2

The index value used to identify the port component (contained in the local chassis with the LLDP agent) associated with this entry. The lldpRemLocalPortNum identifies the port on which the remote system information is received. The value of this object is used as a port index to the lldpRemTable.

lldpRemIndex

OID:1.0.8802.1.1.2.1.4.1.1.3

This object represents an arbitrary local integer value used by this agent to identify a particular connection instance, unique only for the indicated remote system. An agent is encouraged to

assign monotonically increasing index values to new entries, starting with one, after each reboot. It is considered unlikely that the lldpRemIndex will wrap between reboots.

lldpRemChassisIdSubtype

OID:1.0.8802.1.1.2.1.4.1.1.4

The type of encoding used to identify the chassis associated with the remote system. REFERENCE IEEE 802.1AB-2005 9.5.2.2

lldpRemChassisId

OID:1.0.8802.1.1.2.1.4.1.1.5

The type of encoding used to identify the chassis associated with the remote system. REFERENCE IEEE 802.1AB-2005 9.5.2.2

lldpRemPortIdSubtype

OID:1.0.8802.1.1.2.1.4.1.1.6

The type of port identifier encoding used in the associated 'lldpRemPortId' object. REFERENCE IEEE 802.1AB-2005 9.5.3.2

lldpRemPortId

OID:1.0.8802.1.1.2.1.4.1.1.7

The type of port identifier encoding used in the associated 'lldpRemPortId' object. REFERENCE IEEE 802.1AB-2005 9.5.3.2

lldpRemPortDesc

OID:1.0.8802.1.1.2.1.4.1.1.8

The string value used to identify the description of the given port associated with the remote system. REFERENCE IEEE 802.1AB-2005 9.5.5.2

lldpRemSysName

OID:1.0.8802.1.1.2.1.4.1.1.9

The string value used to identify the system name of the remote system. REFERENCE IEEE 802.1AB-2005 9.5.6.2

lldpRemSysDesc

OID:1.0.8802.1.1.2.1.4.1.1.10

The string value used to identify the system description of the remote system. REFERENCE IEEE 802.1AB-2005 9.5.7.2

lldpRemSysCapSupported

OID:1.0.8802.1.1.2.1.4.1.1.11

The bitmap value used to identify which system capabilities are supported on the remote system. REFERENCE IEEE 802.1AB-2005 9.5.8.1

lldpRemSysCapEnabled

OID:1.0.8802.1.1.2.1.4.1.1.12

The bitmap value used to identify which system capabilities are enabled on the remote system. REFERENCE IEEE 802.1AB-2005 9.5.8.2

lldpRemManAddrTable

OID: 1.0.8802.1.1.2.1.4.2

lldpRemManAddrSubtype

OID:1.0.8802.1.1.2.1.4.2.1.1

The type of management address identifier encoding used in the associated 'lldpRemManagmentAddr' object. REFERENCE IEEE 802.1AB-2005 9.5.9.3

lldpRemManAddr

OID:1.0.8802.1.1.2.1.4.2.1.2

This table contains one or more rows per management address information on the remote system learned on a particular port contained in the local chassis known to this agent.

lldpRemManAddrIfSubtype

OID:1.0.8802.1.1.2.1.4.2.1.3

The enumeration value that identifies the interface numbering method used for defining the interface number, associated with the remote system. REFERENCE IEEE 802.1AB-2005 9.5.9.5

lldpRemManAddrIfId

OID:1.0.8802.1.1.2.1.4.2.1.4

The integer value used to identify the interface number regarding the management address component associated with the remote system. REFERENCE IEEE 802.1AB-2005 9.5.9.6

lldpRemManAddrOID

OID:1.0.8802.1.1.2.1.4.2.1.5

The OID value used to identify the type of hardware component or protocol entity associated with the management address advertised by the remote system agent. REFERENCE IEEE 802.1AB-2005 9.5.9.8

system

OID: 1.3.6.1.2.1.1

sysDescr

OID:1.3.6.1.2.1.1.1

A textual description of the entity. This value shouldinclude the full name and version identification ofthe system's hardware type, software operating-system,and networking software.

sysObjectID

OID:1.3.6.1.2.1.1.2

The vendor's authoritative identification of thenetwork management subsystem contained in the entity.This value is allocated within the SMI enterprisessubtree (1.3.6.1.4.1) and provides an easy andunambiguous means for determining what kind of box' isbeing managed. For example, if vendor Flintstones,Inc.' was assigned the subtree 1.3.6.1.4.1.424242,it could assign the identifier 1.3.6.1.4.1.424242.1.1to its Fred Router'.

sysUpTime

OID:1.3.6.1.2.1.1.3

The time (in hundredths of a second) since thenetwork management portion of the system was lastre-initialized.

sysContact

OID:1.3.6.1.2.1.1.4

The textual identification of the contact person forthis managed node, together with information on howto contact this person. If no contact information isknown, the value is the zero-length string.

sysName

OID:1.3.6.1.2.1.1.5

An administratively-assigned name for this managednode. By convention, this is the node's fully-qualifieddomain name. If the name is unknown, the value isthe zero-length string.

sysLocation

OID:1.3.6.1.2.1.1.6

The physical location of this node (e.g., 'telephonecloset, 3rd floor'). If the location is unknown, thevalue is the zero-length string.

sysServices

OID:1.3.6.1.2.1.1.7

A value which indicates the set of services that thisentity may potentially offer. The value is a sum.This sum initially takes the value zero. Then, foreach layer, L, in the range 1 through 7, that this nodeperforms transactions for, 2 raised to (L - 1) is addedto the sum. For example, a node which performs onlyrouting functions would have a value of 4 (2\^(3-1)).In contrast, a node which is a host offering applicationservices would have a value of 72 (2\^(4-1) + 2\^(7-1)).Note that in the context of the Internet suite ofprotocols, values should be calculated accordingly:layer functionality1 physical (e.g., repeaters)2 datalink/subnetwork (e.g., bridges)3 internet (e.g., supports the IP)4 end-to-end (e.g., supports the TCP)7 applications (e.g., supports the SMTP)For systems including OSI protocols, layers 5 and 6may also be counted.

interfaces

OID: 1.3.6.1.2.1.2

ifNumber

OID:1.3.6.1.2.1.2.1

The number of network interfaces (regardless of theircurrent state) present on this system.A list of interface entries. The number of entries isgiven by the value of ifNumber.

ifTable

OID: 1.3.6.1.2.1.2.2

ifIndex

OID:1.3.6.1.2.1.2.2.1.1

A unique value, greater than zero, for each interface. Itis recommended that values are assigned contiguouslystarting from 1. The value for each interface sub-layermust remain constant at least from one re-initialization ofthe entity's network management system to the next re-initialization.

ifDescr

OID:1.3.6.1.2.1.2.2.1.2

A textual string containing information about theinterface. This string should include the name of themanufacturer, the product name and the version of theinterface hardware/software.

ifType

OID:1.3.6.1.2.1.2.2.1.3

The type of interface. Additional values for ifType areassigned by the Internet Assigned Numbers Authority (IANA),through updating the syntax of the IANAifType textualconvention.

ifMtu

OID:1.3.6.1.2.1.2.2.1.4

The size of the largest packet which can be sent/receivedon the interface, specified in octets. For interfaces thatare used for transmitting network datagrams, this is thesize of the largest network datagram that can be sent on theinterface.

ifSpeed

OID:1.3.6.1.2.1.2.2.1.5

An estimate of the interface's current bandwidth in bitsper second. For interfaces which do not vary in bandwidthor for those where no accurate estimation can be made, thisobject should contain the

nominal bandwidth. If thebandwidth of the interface is greater than the maximum valuereportable by this object then this object should report itsmaximum value (4,294,967,295) and ifHighSpeed must be usedto report the interace's speed. For a sub-layer which hasno concept of bandwidth, this object should be zero.

ifPhysAddress

OID:1.3.6.1.2.1.2.2.1.6

The interface's address at its protocol sub-layer. Forexample, for an 802.x interface, this object normallycontains a MAC address. The interface's media-specific MIBmust define the bit and byte ordering and the format of thevalue of this object. For interfaces which do not have suchan address (e.g., a serial line), this object should containan octet string of zero length.

ifAdminStatus

OID:1.3.6.1.2.1.2.2.1.7

The desired state of the interface. The testing(3) stateindicates that no operational packets can be passed. When amanaged system initializes, all interfaces start withifAdminStatus in the down(2) state. As a result of eitherexplicit management action or per configuration informationretained by the managed system, ifAdminStatus is thenchanged to either the up(1) or testing(3) states (or remainsin the down(2) state).

ifOperStatus

OID:1.3.6.1.2.1.2.2.1.8

The current operational state of the interface. Thetesting(3) state indicates that no operational packets canbe passed. If ifAdminStatus is down(2) then ifOperStatusshould be down(2). If ifAdminStatus is changed to up(1)then ifOperStatus should change to up(1) if the interface isready to transmit and receive network traffic; it shouldchange to dormant(5) if the interface is waiting forexternal actions (such as a serial line waiting for anincoming connection); it should remain in the down(2) stateif and only if there is a fault that prevents it from goingto the up(1) state; it should remain in the notPresent(6)state if the interface has missing (typically, hardware)components.

ifLastChange

OID:1.3.6.1.2.1.2.2.1.9

The value of sysUpTime at the time the interface enteredits current operational state. If the current state wasentered prior to the last re-initialization of the localnetwork management subsystem, then this object contains azero value.

ifInOctets

OID:1.3.6.1.2.1.2.2.1.10

The total number of octets received on the interface,including framing characters.Discontinuities in the value of this counter can occur atre-initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifInUcastPkts

OID:1.3.6.1.2.1.2.2.1.11

The number of packets, delivered by this sub-layer to ahigher (sub-)layer, which were not addressed to a multicastor broadcast address at this sub-layer.Discontinuities in the value of this counter can occur atre-initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifInNUcastPkts

OID:1.3.6.1.2.1.2.2.1.12

ifInDiscards

OID:1.3.6.1.2.1.2.2.1.13

The number of inbound packets which were chosen to bediscarded even though no errors had been detected to preventtheir being deliverable to a higher-layer protocol. Onepossible reason for discarding such a packet could be tofree up buffer space.Discontinuities in the value of this counter can occur atre-initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifInErrors

OID:1.3.6.1.2.1.2.2.1.14

For packet-oriented interfaces, the number of inboundpackets that contained errors preventing them from beingdeliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inboundtransmission units that contained errors preventing themfrom being deliverable to a higher-layer protocol.Discontinuities in the value of this counter can occur

atre-initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifInUnknownProtos

OID:1.3.6.1.2.1.2.2.1.15

For packet-oriented interfaces, the number of packetsreceived via the interface which were discarded because ofan unknown or unsupported protocol. For character-orientedor fixed-length interfaces that support protocolmultiplexing the number of transmission units received viathe interface which were discarded because of an unknown orunsupported protocol. For any interface that does notsupport protocol multiplexing, this counter will always be0.Discontinuities in the value of this counter can occur atre-initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifOutOctets

OID:1.3.6.1.2.1.2.2.1.16

The total number of octets transmitted out of theinterface, including framing characters.Discontinuities in the value of this counter can occur atre-initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifOutUcastPkts

OID:1.3.6.1.2.1.2.2.1.17

The total number of packets that higher-level protocolsrequested be transmitted, and which were not addressed to amulticast or broadcast address at this sub-layer, includingthose that were discarded or not sent.Discontinuities in the value of this counter can occur atre-initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifOutNUcastPkts

OID:1.3.6.1.2.1.2.2.1.18

ifOutDiscards

OID:1.3.6.1.2.1.2.2.1.19

The number of outbound packets which were chosen to bediscarded even though no errors had been detected to preventtheir being transmitted. One possible reason for discardingsuch a packet could be to free up buffer space.Discontinuities in the value of this counter can occur atre-

initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifOutErrors

OID:1.3.6.1.2.1.2.2.1.20

For packet-oriented interfaces, the number of outboundpackets that could not be transmitted because of errors.For character-oriented or fixed-length interfaces, thenumber of outbound transmission units that could not betransmitted because of errors.Discontinuities in the value of this counter can occur atre-initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifOutQLen

OID:1.3.6.1.2.1.2.2.1.21

ifSpecific

OID:1.3.6.1.2.1.2.2.1.22

icmp

OID: 1.3.6.1.2.1.5

icmpInMsgs

OID:1.3.6.1.2.1.5.1

Total number of ICMP messages which the entity received. Note that this counter includes all those counted by icmpInErrors.

icmpInErrors

OID:1.3.6.1.2.1.5.2

Number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length…

icmpInDestUnreachs

OID:1.3.6.1.2.1.5.3

Number of ICMP Destination Unreachable messages received.

icmpInTimeExcds

OID:1.3.6.1.2.1.5.4

Number of ICMP Time Exceeded messages received.

icmpInParmProbs

OID:1.3.6.1.2.1.5.5

Number of ICMP Parameter Problem messages received.

icmpInSrcQuenchs

OID:1.3.6.1.2.1.5.6

Number of ICMP Source Quench messages received.

icmpInRedirects

OID:1.3.6.1.2.1.5.7

icmpInEchos

OID:1.3.6.1.2.1.5.8

Number of ICMP Echo (request) messages received.

icmpInEchoReps

OID:1.3.6.1.2.1.5.9

Number of ICMP Echo Reply messages received.

icmpInTimestamps

OID:1.3.6.1.2.1.5.10

Number of ICMP Timestamp (request) messages received.

icmpInTimestampReps

OID:1.3.6.1.2.1.5.11

Number of ICMP Timestamp Reply messages received.

icmpInAddrMasks

OID:1.3.6.1.2.1.5.12

Number of ICMP Address Mask Request messages received.

icmpInAddrMaskReps

OID:1.3.6.1.2.1.5.13

Number of ICMP Address Mask Reply messages received.

icmpOutMsgs

OID:1.3.6.1.2.1.5.14

Total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by icmpOut…

icmpOutErrors

OID:1.3.6.1.2.1.5.15

Number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This v…

icmpOutDestUnreachs

OID:1.3.6.1.2.1.5.16

The number of ICMP Destination Unreachablemessages sent.

icmpOutTimeExcds

OID:1.3.6.1.2.1.5.17

The number of ICMP Time Exceeded messages sent.

icmpOutParmProbs

OID:1.3.6.1.2.1.5.18

The number of ICMP Parameter Problem messagessent.

icmpOutSrcQuenchs

OID:1.3.6.1.2.1.5.19

The number of ICMP Source Quench messages sent.

icmpOutRedirects

OID:1.3.6.1.2.1.5.20

The number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.

icmpOutEchos

OID:1.3.6.1.2.1.5.21

The number of ICMP Echo (request) messages sent.

icmpOutEchoReps

OID:1.3.6.1.2.1.5.22

The number of ICMP Echo Reply messages sent.

icmpOutTimestamps

OID:1.3.6.1.2.1.5.23

The number of ICMP Timestamp (request) messages sent

icmpOutTimestampReps

OID:1.3.6.1.2.1.5.24

The number of ICMP Timestamp Reply messages sent

icmpOutAddrMasks

OID:1.3.6.1.2.1.5.25

The number of ICMP Address Mask Request messages sent

icmpOutAddrMaskReps

OID:1.3.6.1.2.1.5.26

The number of ICMP Address Mask Reply messages sent

udp

OID: 1.3.6.1.2.1.7

udpInDatagrams

OID:1.3.6.1.2.1.7.1

The total number of UDP datagrams delivered to UDPusers.Discontinuities in the value of this counter can occurat re-initialization of the management system, and atother times as indicated by discontinuities in thevalue of sysUpTime.

udpNoPorts

OID:1.3.6.1.2.1.7.2

The total number of received UDP datagrams for whichthere was no application at the destination port.Discontinuities in the value of this counter can occurat re-initialization of the management system, and atother times as indicated by discontinuities in thevalue of sysUpTime.

udpInErrors

OID:1.3.6.1.2.1.7.3

The number of received UDP datagrams that could not bedelivered for reasons other than the lack of anapplication at the destination port.Discontinuities in the value of this counter can occurat re-initialization of the management system, and atother times as indicated by discontinuities in thevalue of sysUpTime.

udpOutDatagrams

OID:1.3.6.1.2.1.7.4

The total number of UDP datagrams sent from thisentity.Discontinuities in the value of this counter can occurat re-initialization of the management system, and atother times as indicated by discontinuities in thevalue of sysUpTime.

udpTable

OID: 1.3.6.1.2.1.7.5

udpLocalAddress

OID:1.3.6.1.2.1.7.5.1.1

The local IP address for this UDP listener. In the case of a UDP listener that is willing to accept datagrams for any IP interface associated with the node, the value 0.0.0.0 is used.

udpLocalPort

OID:1.3.6.1.2.1.7.5.1.2

The local port number for this UDP listener.

snmp

OID: 1.3.6.1.2.1.11

snmpInPkts

OID:1.3.6.1.2.1.11.1

The total number of messages delivered to the SNMPentity from the transport service.

snmpInBadVersions

OID:1.3.6.1.2.1.11.3

The total number of SNMP messages which were deliveredto the SNMP entity and were for an unsupported SNMPversion.

snmpInBadCommunityNames

OID:1.3.6.1.2.1.11.4

The total number of community-based SNMP messages (forexample, SNMPv1) delivered to the SNMP entity whichused an SNMP community name not known to said entity.Also, implementations which authenticate community-basedSNMP messages using check(s) in addition to matchingthe community name (for example, by also checkingwhether the message originated from a transport addressallowed to use a specified community name) MAY includein this value the number of messages which failed theadditional check(s). It is strongly RECOMMENDED thatthe documentation for any security model which is usedto authenticate community-based SNMP messages specifythe precise conditions that contribute to this value.

snmpInBadCommunityUses

OID:1.3.6.1.2.1.11.5

The total number of community-based SNMP messages (forexample, SNMPv1) delivered to the SNMP entity whichrepresented an SNMP operation that was not allowed forthe SNMP community named in the message. The preciseconditions under which this counter is incremented(if at all) depend on how the SNMP entity implementsits access control mechanism and how its applicationsinteract with that access control mechanism. It isstrongly RECOMMENDED that the documentation for anyaccess control mechanism which is used to control accessto and visibility of MIB instrumentation specify theprecise conditions that contribute to this value.

snmpInASNParseErrs

OID:1.3.6.1.2.1.11.6

The total number of ASN.1 or BER errors encountered bythe SNMP entity when decoding received SNMP messages.

snmpEnableAuthenTraps

OID:1.3.6.1.2.1.11.30

Indicates whether the SNMP entity is permitted togenerate authenticationFailure traps. The value of thisobject overrides any configuration information; as such,it provides a means whereby all authenticationFailuretraps may be disabled.Note that it is strongly recommended that this objectbe stored in non-volatile memory so that it remainsconstant across re-initializations of the networkmanagement system.

snmpSilentDrops

OID:1.3.6.1.2.1.11.31

The total number of Confirmed Class PDUs (such asGetRequest-PDUs, GetNextRequest-PDUs,GetBulkRequest-PDUs, SetRequest-PDUs, andInformRequest-PDUs) delivered to the SNMP entity whichwere silently dropped because the size of a replycontaining an alternate Response Class PDU (such as aResponse-PDU) with an empty variable-bindings fieldwas greater than either a local constraint or themaximum message size associated with the originator ofthe request.

snmpProxyDrops

OID:1.3.6.1.2.1.11.32

The total number of Confirmed Class PDUs(such as GetRequest-PDUs, GetNextRequest-PDUs,GetBulkRequest-PDUs, SetRequest-PDUs, andInformRequest-PDUs) delivered to the SNMP entity whichwere silently dropped because the transmission ofthe (possibly translated) message to a proxy targetfailed in a manner (other than a time-out) such thatno Response Class PDU (such as a Response-PDU) couldbe returned.

ifMIBObjects

OID: 1.3.6.1.2.1.31.1

ifXTable

OID: 1.3.6.1.2.1.31.1.1

ifNamed

OID:1.3.6.1.2.1.31.1.1.1.1

The textual name of the interface. The value of this object should be the name of the interface as assigned by the local device and should be suitable for use in commands entered at the device's console'. This might be a text name, such as le0' or a simple port number, such as 1', depending on the interface naming syntax of the device. If several entries in the ifTable together represent a single interface as named by the device, then each will have the same value of ifName. Note that for an agent which responds to SNMP queries concerning an interface on some other (proxied) device, then the value of ifName for such an interface is the proxied device's local name for it. If there is no local name, or this object is otherwise not applicable, then this object contains a zero-length string.

ifInMulticastPkts

OID:1.3.6.1.2.1.31.1.1.1.2

The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer. For a MAC layer protocol, this includes both Group and Functional addresses. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

ifInBroadcastPkts

OID:1.3.6.1.2.1.31.1.1.1.3

The number of packets, delivered by this sub-layer to ahigher (sub-)layer, which were addressed to a broadcastaddress at this sub-layer.Discontinuities in the value of this counter can occur atre-initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifOutMulticastPkts

OID:1.3.6.1.2.1.31.1.1.1.4

The total number of packets that higher-level protocolsrequested be transmitted, and which were addressed to amulticast address at this sub-layer, including those thatwere discarded or not sent. For a MAC layer protocol, thisincludes both Group and Functional addresses.Discontinuities in the value of this counter can occur atre-initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifOutBroadcastPkts

OID:1.3.6.1.2.1.31.1.1.1.5

The total number of packets that higher-level protocolsrequested be transmitted, and which were addressed to abroadcast address at this sub-layer, including those thatwere discarded or not sent.Discontinuities in the value of this counter can occur atre-initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifHCInOctets

OID:1.3.6.1.2.1.31.1.1.1.6

The total number of octets received on the interface,including framing characters. This object is a 64-bitversion of ifInOctets.Discontinuities in the value of this counter can occur atre-initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifHCInUcastPkts

OID:1.3.6.1.2.1.31.1.1.1.7

The number of packets, delivered by this sub-layer to ahigher (sub-)layer, which were not addressed to a multicastor broadcast address at this sub-layer. This object is a64-bit version of ifInUcastPkts.Discontinuities in the value of this counter can occur atre-initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifHCInMulticastPkts

OID:1.3.6.1.2.1.31.1.1.1.8

The number of packets, delivered by this sub-layer to ahigher (sub-)layer, which were addressed to a multicastaddress at this sub-layer. For a MAC layer protocol, thisincludes both Group and Functional addresses. This objectis a 64-bit version of ifInMulticastPkts.Discontinuities in the value of this counter can occur atre-initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifHCInBroadcastPkts

OID:1.3.6.1.2.1.31.1.1.1.9

The number of packets, delivered by this sub-layer to ahigher (sub-)layer, which were addressed to a broadcastaddress at this sub-layer. This object is a 64-bit versionof ifInBroadcastPkts.Discontinuities in the value of this counter can occur atre-initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifHCOutOctets

OID:1.3.6.1.2.1.31.1.1.1.10

The total number of octets transmitted out of theinterface, including framing characters. This object is a64-bit version of ifOutOctets.Discontinuities in the value of this counter can occur atre-initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifHCOutUcastPkts

OID:1.3.6.1.2.1.31.1.1.1.11

The total number of packets that higher-level protocolsrequested be transmitted, and which were not addressed to amulticast or broadcast address at this sub-layer, includingthose that were discarded or not sent. This object is a64-bit version of ifOutUcastPkts.Discontinuities in the value of this counter can occur atre-initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifHCOutMulticastPkts

OID:1.3.6.1.2.1.31.1.1.1.12

The total number of packets that higher-level protocolsrequested be transmitted, and which were addressed to amulticast address at this sub-layer, including those thatwere discarded or not sent. For a MAC layer protocol, thisincludes both Group and Functional addresses. This objectis a 64-bit version of ifOutMulticastPkts.Discontinuities in the value of this counter can occur atre-initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifHCOutBroadcastPkts

OID:1.3.6.1.2.1.31.1.1.1.13

The total number of packets that higher-level protocolsrequested be transmitted, and which were addressed to abroadcast address at this sub-layer, including those thatwere discarded or not sent. This object is a 64-bit versionof ifOutBroadcastPkts.Discontinuities in the value of this counter can occur atre-initialization of the management system, and at othertimes as indicated by the value ofifCounterDiscontinuityTime.

ifLinkUpDownTrapEnable

OID:1.3.6.1.2.1.31.1.1.1.14

Indicates whether linkUp/linkDown traps should be generatedfor this interface.By default, this object should have the value enabled(1) forinterfaces which do not operate on 'top' of any otherinterface (as defined in the ifStackTable), and disabled(2)otherwise.

ifHighSpeed

OID:1.3.6.1.2.1.31.1.1.1.15

An estimate of the interface's current bandwidth in unitsof 1,000,000 bits per second. If this object reports avalue of n' then the speed of the interface is somewhere inthe range of n-500,000' to n+499,999'. For interfaceswhich do not vary in bandwidth or for those where noaccurate estimation can be made, this object should containthe nominal bandwidth. For a sub-layer which has no conceptof bandwidth, this object should be zero.

ifPromiscuousMode

OID:1.3.6.1.2.1.31.1.1.1.16

This object has a value of false(2) if this interface onlyaccepts packets/frames that are addressed to this station.This object has a value of true(1) when the station acceptsall packets/frames transmitted on the media. The valuetrue(1) is only legal on certain types of media. If legal,setting

this object to a value of true(1) may require theinterface to be reset before becoming effective.The value of ifPromiscuousMode does not affect the receptionof broadcast and multicast packets/ frames by the interface.

ifConnectorPresent

OID:1.3.6.1.2.1.31.1.1.1.17

This object has the value 'true(1)' if the interfacesublayer has a physical connector and the value 'false(2)'otherwise.

ifAlias

OID:1.3.6.1.2.1.31.1.1.1.18

This object is an 'alias' name for the interface asspecified by a network manager, and provides a non-volatile'handle' for the interface.On the first instantiation of an interface, the value ofifAlias associated with that interface is the zero-lengthstring. As and when a value is written into an instance ofifAlias through a network management set operation, then theagent must retain the supplied value in the ifAlias instanceassociated with the same interface for as long as thatinterface remains instantiated, including across all re-initializations/reboots of the network management system,including those which result in a change of the interface'sifIndex value.An example of the value which a network manager might storein this object for a WAN interface is the (Telco's) circuitnumber/identifier of the interface.Some agents may support write-access only for interfaceshaving particular values of ifType. An agent which supportswrite access to this object is required to keep the value innon-volatile storage, but it may limit the length of newvalues depending on how much storage is already occupied bythe current values for other interfaces.

ifCounterDiscontinuityTime

OID:1.3.6.1.2.1.31.1.1.1.19

The value of sysUpTime on the most recent occasion at whichany one or more of this interface's counters suffered adiscontinuity. The relevant counters are the specificinstances associated with this interface of any Counter32 orCounter64 object contained in the ifTable or ifXTable. Ifno such discontinuities have occurred since the last re-initialization of the local management subsystem, then thisobject contains a zero value.

ifTableLastChange

OID:1.3.6.1.2.1.31.1.5

The value of sysUpTime at the time of the last creation ordeletion of an entry in the ifTable. If the number ofentries has been unchanged since the last re-initializationof the local network management subsystem, then this objectcontains a zero value.A list of interface entries. The number of entries isgiven by the value of ifNumber. This table containsadditional objects for the interface table.

[

Citrix ADC Enterprise OIDs

‹ Citrix ADC SNMP OID Reference

Citrix ADC Enterprise OIDs

nsSysGroup

OID: 1.3.6.1.4.1.5951.4.1.1 This provides information about the system properties of Netscaler product.

sysBuildVersion

OID: 1.3.6.1.4.1.5951.4.1.1.1 This shows the version of the kernel build running on the Citrix ADC.

sysIpAddress

OID: 1.3.6.1.4.1.5951.4.1.1.2 This shows the configured ipaddress of the Citrix ADC

sysNetmask

OID: 1.3.6.1.4.1.5951.4.1.1.3 This shows the configured netmask of the Citrix ADC

sysHighAvailabilityMode

OID: 1.3.6.1.4.1.5951.4.1.1.6 This shows whether Citrix ADC is in standalone mode or whether it is primary or secondary in case of failover mode.

sysGateway

OID: 1.3.6.1.4.1.5951.4.1.1.7 This represents the default gateway configured on the Citrix ADC

sysCurMappedIpCount

OID: 1.3.6.1.4.1.5951.4.1.1.8 This represents the number of Mapped IPs currently configured on the Citrix ADC system

sysCustomID

OID: 1.3.6.1.4.1.5951.4.1.1.9 Configurable Identifier for the system

sysHardwareVersionId

OID: 1.3.6.1.4.1.5951.4.1.1.10 The hardware version ID of the Citrix ADC system

sysHardwareVersionDesc

OID: 1.3.6.1.4.1.5951.4.1.1.11 The hardware version description of the Citrix ADC system

sysTotConfigChanges

OID: 1.3.6.1.4.1.5951.4.1.1.12 The number of times a configuration change was made on the Citrix ADC.

sysTotSaveConfigs

OID: 1.3.6.1.4.1.5951.4.1.1.13 Number of times the system configuration was saved on the Citrix ADC.

sysHardwareSerialNumber

OID: 1.3.6.1.4.1.5951.4.1.1.14 The serial number of the Citrix ADC system.

sysHardwareEncodedSerialNumber

OID: 1.3.6.1.4.1.5951.4.1.1.15 The encoded serial no of the Citrix ADC system.

sysModelId

OID: 1.3.6.1.4.1.5951.4.1.1.16 The model ID is populated if the system is such that it is license controlled. If the system does not support license based models, then the model id will be zero.

nsFeatureInfo

OID: 1.3.6.1.4.1.5951.4.1.1.20 This provides information about the various features in the Netscaler product.

featureWebLogging

OID: 1.3.6.1.4.1.5951.4.1.1.20.1 This represents whether webLogging feature is enabled or disabled on Citrix ADC.

featureSurgeProtection

OID: 1.3.6.1.4.1.5951.4.1.1.20.2 This represents whether surgeProtection feature is enabled or disabled on Citrix ADC .

featureLoadBalancing

OID: 1.3.6.1.4.1.5951.4.1.1.20.3 This represents whether LoadBalancing feature is enabled or disabled on Citrix ADC .

featureContentSwitching

OID: 1.3.6.1.4.1.5951.4.1.1.20.4 This represents whether contentSwitching feature is enabled or disabled on Citrix ADC .

featureCacheRedirection

OID: 1.3.6.1.4.1.5951.4.1.1.20.5 This represents whether cacheRedirection feature is enabled or disabled on Citrix ADC .

featureSureConnect

OID: 1.3.6.1.4.1.5951.4.1.1.20.6 This represents whether sureConnect feature is enabled or disabled on Citrix ADC .

featureCompression

OID: 1.3.6.1.4.1.5951.4.1.1.20.7 This represents whether compression feature is enabled or disabled on Citrix ADC .

featurePriorityQueuing

OID: 1.3.6.1.4.1.5951.4.1.1.20.8 This represents whether priorityQueuing feature is enabled or disabled on Citrix ADC .

featureSslOffloading

OID: 1.3.6.1.4.1.5951.4.1.1.20.9 This represents whether sslOffloading feature is enabled or disabled on Citrix ADC .

featureGslb

OID: 1.3.6.1.4.1.5951.4.1.1.20.10 This represents whether gslb feature is enabled or disabled on Citrix ADC .

featureHttpDosProtection

OID: 1.3.6.1.4.1.5951.4.1.1.20.11 This represents whether httpDosProtection feature is enabled or disabled on Citrix ADC .

featureInternalCaching

OID: 1.3.6.1.4.1.5951.4.1.1.20.14 This represents whether internalCaching feature is enabled or disabled on Citrix ADC .

featureSSLVPN

OID: 1.3.6.1.4.1.5951.4.1.1.20.15 This represents whether SSL VPN feature is enabled or disabled on Citrix ADC .

featureOSPF

OID: 1.3.6.1.4.1.5951.4.1.1.20.16 This represents whether OSPF feature is enabled or disabled on Citrix ADC .

featureRIP

OID: 1.3.6.1.4.1.5951.4.1.1.20.17 This represents whether RIP feature is enabled or disabled on Citrix ADC .

featureBGP

OID: 1.3.6.1.4.1.5951.4.1.1.20.18 This represents whether BGP feature is enabled or disabled on Citrix ADC .

featureRewrite

OID: 1.3.6.1.4.1.5951.4.1.1.20.19 This represents whether Rewrite feature is enabled or disabled on Citrix ADC .

featureDeltaCompression

OID: 1.3.6.1.4.1.5951.4.1.1.20.20 This represents whether Delta Compression feature is enabled or disabled on Citrix ADC .

featureGSLBProximity

OID: 1.3.6.1.4.1.5951.4.1.1.20.21 This represents whether GSLB Proximity feature is enabled or disabled on Citrix ADC .

featureIPv6ProtocolTranslation

OID: 1.3.6.1.4.1.5951.4.1.1.20.22 This represents whether IPv6 Protocol Translation feature is enabled or disabled on Citrix ADC .

featureApplicationFirewall

OID: 1.3.6.1.4.1.5951.4.1.1.20.23 This represents whether Application Firewall feature is enabled or disabled on Citrix ADC .

featureResponder

OID: 1.3.6.1.4.1.5951.4.1.1.20.24 This represents whether Responder feature is enabled or disabled on Citrix ADC .

featureAGEE

OID: 1.3.6.1.4.1.5951.4.1.1.20.50 This represents whether AGEE feature of SSLVPN is enabled or disabled on Citrix ADC .

featureAAA

OID: 1.3.6.1.4.1.5951.4.1.1.20.51 This represents whether Authentication, Authorization and Auditing features for Traffic Management vservers are enabled or disabled on Citrix ADC .

featurePLATFORM

OID: 1.3.6.1.4.1.5951.4.1.1.20.60 This gives platform information AGEE 1 NSVA 2 etc

featureAPPFLOW

OID: 1.3.6.1.4.1.5951.4.1.1.20.61 This represents whether APPFLOW feature is enabled or disable on Citrix ADC .

featureISIS

OID: 1.3.6.1.4.1.5951.4.1.1.20.62 This represents whether ISIS feature is enabled or disabled on Citrix ADC .

nsModeInfo

OID: 1.3.6.1.4.1.5951.4.1.1.21 This provides information about the mode a certain feature is in, in the Netscaler product.

modeFastRamp

OID: 1.3.6.1.4.1.5951.4.1.1.21.1 This represents whether fastRamp mode is enabled or disabled on Citrix ADC .

l2Mode

OID: 1.3.6.1.4.1.5951.4.1.1.21.2 This represents whether l2Mode mode is enabled or disabled on Citrix ADC .

modeUseSrcIp

OID: 1.3.6.1.4.1.5951.4.1.1.21.3 This represents whether useSrcIp mode is enabled or disabled on Citrix ADC .

modeClientKeepAlive

OID: 1.3.6.1.4.1.5951.4.1.1.21.4 This represents whether clientKeepAlive mode is enabled or disabled on Citrix ADC .

modeTcpBuffering

OID: 1.3.6.1.4.1.5951.4.1.1.21.5 This represents whether tcpBuffering mode is enabled or disabled on Citrix ADC .

modeMacBasedForwarding

OID: 1.3.6.1.4.1.5951.4.1.1.21.6 This represents whether macBasedForwarding mode is enabled or disabled on Citrix ADC .

modeUseSubnetIp

OID: 1.3.6.1.4.1.5951.4.1.1.21.7 This represents whether Use Subnet IP mode is enabled or disabled on Citrix ADC .

modeEdgeConfiguration

OID: 1.3.6.1.4.1.5951.4.1.1.21.8 This represents whether Edge Configuration mode is enabled or disabled on Citrix ADC .

l3mode

OID: 1.3.6.1.4.1.5951.4.1.1.21.9 This represents whether l3 mode (ip forwarding) is enabled or disabled on Citrix ADC .

modePathMTUDiscovery

OID: 1.3.6.1.4.1.5951.4.1.1.21.10 This represents whether path MTU discovery mode is enabled or disabled on Citrix ADC .

modeStaticRouteAdv

OID: 1.3.6.1.4.1.5951.4.1.1.21.11 This represents whether static route advertisement mode is enabled or disabled on Citrix ADC .

modeDirectRouteAdv

OID: 1.3.6.1.4.1.5951.4.1.1.21.12 This represents whether direct route advertisement mode is enabled or disabled on Citrix ADC .

modeIntranetRouteAdv

OID: 1.3.6.1.4.1.5951.4.1.1.21.13 This represents whether intranet route advertisement mode is enabled or disabled on Citrix ADC .

brgBpdu

OID: 1.3.6.1.4.1.5951.4.1.1.21.14 This represents whether Bridging of BPDU is enabled or disabled on Citrix ADC .

modeIpv6StaticRouteAdv

OID: 1.3.6.1.4.1.5951.4.1.1.21.15 This represents whether Ipv6 static route advertisement mode is enabled or disabled on Citrix ADC .

modeIpv6DirectRouteAdv

OID: 1.3.6.1.4.1.5951.4.1.1.21.16 This represents whether Ipv6 direct route advertisement mode is enabled or disabled on Citrix ADC .

mediaclassification

OID: 1.3.6.1.4.1.5951.4.1.1.21.17 This represents whether mediaclassification mode is enabled or disabled on Citrix ADC .

aclStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.22.1 This provides statistical information about the configured ACLs in the Netscaler product.

aclTotPktsBridged

OID: 1.3.6.1.4.1.5951.4.1.1.22.1.9 Packets matching a bridge ACL, which is in transparent mode and bypasses service processing.

aclTotPktsDenied

OID: 1.3.6.1.4.1.5951.4.1.1.22.1.10 Packets dropped because they match ACLs with processing mode set to DENY.

aclTotPktsAllowed

OID: 1.3.6.1.4.1.5951.4.1.1.22.1.11 Packets matching ACLs with processing mode set to ALLOW. Citrix ADC processes these packets.

aclTotHits

OID: 1.3.6.1.4.1.5951.4.1.1.22.1.12 Packets matching an ACL.

aclTotMisses

OID: 1.3.6.1.4.1.5951.4.1.1.22.1.13 Packets not matching any ACL.

aclTotPktsNAT

OID: 1.3.6.1.4.1.5951.4.1.1.22.1.14 Packets matching a NAT ACL, resulting in a NAT session.

nsAclTable

OID: 1.3.6.1.4.1.5951.4.1.1.22.1.20 This table contains all the ACLs configured This is indexed on the aclName See "Citrix ADC Enterprise OIDs" on page 37 See "Citrix ADC Enterprise OIDs" on page 37 See "Citrix ADC Enterprise OIDs" on page 37 See "Citrix ADC Enterprise OIDs" on page 37 .

aclName

OID: 1.3.6.1.4.1.5951.4.1.1.22.1.20.1.1 The name of the ACL

aclPriority

OID: 1.3.6.1.4.1.5951.4.1.1.22.1.20.1.2 The priority of the ACL

aclperHits

OID: 1.3.6.1.4.1.5951.4.1.1.22.1.20.1.4 Number of times the acl was hit

aclFullName

OID: 1.3.6.1.4.1.5951.4.1.1.22.1.20.1.5 The full name of the ACL

aclTotCount

OID: 1.3.6.1.4.1.5951.4.1.1.22.1.21 Total number of ACL rules configured.

dfdaclTotCount

OID: 1.3.6.1.4.1.5951.4.1.1.22.1.22 Total number of DFD ACL rules configured.

dfdaclTotHits

OID: 1.3.6.1.4.1.5951.4.1.1.22.1.23 Packets matching an dfd ACL.

dfdaclTotMisses

OID: 1.3.6.1.4.1.5951.4.1.1.22.1.24 Packets not matching any DFD ACL.

effectiveAclTotCount

OID: 1.3.6.1.4.1.5951.4.1.1.22.1.25 Total number of Effective ACL rules configured.

saclStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.22.3 This provides statistical information about the configured SimpleACLs in the Netscaler product.

saclTotPktsBridged

OID: 1.3.6.1.4.1.5951.4.1.1.22.3.1 Total packets that matched a SimpleACL with action BRIDGE and got bridged by Citrix ADC.

saclTotPktsDenied

OID: 1.3.6.1.4.1.5951.4.1.1.22.3.2 Packets dropped because they match SimpleACL (Access Control List) with processing mode set to DENY.

saclTotPktsAllowed

OID: 1.3.6.1.4.1.5951.4.1.1.22.3.3 Total packets that matched a SimpleACL with action ALLOW and got consumed by Citrix ADC.

saclTotHits

OID: 1.3.6.1.4.1.5951.4.1.1.22.3.4 Packets matching a SimpleACL.

saclTotMisses

OID: 1.3.6.1.4.1.5951.4.1.1.22.3.5 Packets not matching any SimpleACL.

saclsCount

OID: 1.3.6.1.4.1.5951.4.1.1.22.3.6 Number of SimpleACLs configured.

acl6StatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.22.4 This provides statistical information about the configured ACLs6 in the Netscaler product.

nsAcl6Table

OID: 1.3.6.1.4.1.5951.4.1.1.22.4.20 This table contains all the ACLs6 configured This is indexed on the acAclName .

acAclName

OID: 1.3.6.1.4.1.5951.4.1.1.22.4.20.1.1 The name of the ACL6

acl6Priority

OID: 1.3.6.1.4.1.5951.4.1.1.22.4.20.1.2 The priority of the ACL6

acl6perHits

OID: 1.3.6.1.4.1.5951.4.1.1.22.4.20.1.3 Number of times the acl6 was hit

acl6FullName

OID: 1.3.6.1.4.1.5951.4.1.1.22.4.20.1.4 The full name of the ACL6

acl6TotPktsBridged

OID: 1.3.6.1.4.1.5951.4.1.1.22.4.21 Packets matching a bridge IPv6 ACL, which is in transparent mode and bypasses service processing.

acl6TotPktsDenied

OID: 1.3.6.1.4.1.5951.4.1.1.22.4.22 Packets dropped because they match IPv6 ACLs with processing mode set to DENY.

acl6TotPktsAllowed

OID: 1.3.6.1.4.1.5951.4.1.1.22.4.23 Packets matching IPv6 ACLs with processing mode set to ALLOW. Citrix ADC processes these packets.

acl6TotPktsNAT

OID: 1.3.6.1.4.1.5951.4.1.1.22.4.24 Packets matching a NAT ACL6, resulting in a NAT session.

acl6TotHits

OID: 1.3.6.1.4.1.5951.4.1.1.22.4.25 Packets matching an IPv6 ACL.

acl6TotMisses

OID: 1.3.6.1.4.1.5951.4.1.1.22.4.26 Packets not matching any IPv6 ACL.

acl6TotPktsNAT64

OID: 1.3.6.1.4.1.5951.4.1.1.22.4.27 Packets matching a NAT64 ACL6, resulting in a NAT64 translation.

acl6TotCount

OID: 1.3.6.1.4.1.5951.4.1.1.22.4.28 Total number of ACL6 rules configured.

dfdacl6TotCount

OID: 1.3.6.1.4.1.5951.4.1.1.22.4.29 Total number of DFD ACL6 rules configured.

dfdacl6TotHits

OID: 1.3.6.1.4.1.5951.4.1.1.22.4.30 Packets matching an dfd ACL6.

dfdacl6TotMisses

OID: 1.3.6.1.4.1.5951.4.1.1.22.4.31 Packets not matching any DFD ACL6.

pbrStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.22.5 This provides statistical information about the configured PBRs in the Netscaler product.

nsPbrTable

OID: 1.3.6.1.4.1.5951.4.1.1.22.5.20 This table contains all the PBRs configured This is indexed on the pbrName.

pbrName

OID: 1.3.6.1.4.1.5951.4.1.1.22.5.20.1.1 The name of the PBR

pbrFullName

OID: 1.3.6.1.4.1.5951.4.1.1.22.5.20.1.2 The Full name of the PBR

pbrPriority

OID: 1.3.6.1.4.1.5951.4.1.1.22.5.20.1.3 The priority of the PBR

pbrperHits

OID: 1.3.6.1.4.1.5951.4.1.1.22.5.20.1.4 Number of times the pbr was hit

pbrTotPktsAllowed

OID: 1.3.6.1.4.1.5951.4.1.1.22.5.21 Total packets that matched the PBR (Policy-Based Routes) with action ALLOW

pbrTotPktsDenied

OID: 1.3.6.1.4.1.5951.4.1.1.22.5.22 Total packets that matched the PBR with action DENY

pbrTotHits

OID: 1.3.6.1.4.1.5951.4.1.1.22.5.23 Total packets that matched one of the configured PBR

pbrTotMisses

OID: 1.3.6.1.4.1.5951.4.1.1.22.5.24 Total packets that did not match any PBR

pbrTotNullDrop

OID: 1.3.6.1.4.1.5951.4.1.1.22.5.25 Total packets that are dropped due to null nexthop

sacl6StatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.22.6 This provides statistical information about the configured SimpleACL6s in the Netscaler product.

sacl6TotPktsBridged

OID: 1.3.6.1.4.1.5951.4.1.1.22.6.1 Total packets that matched a SimpleACL6 with action BRIDGE and got bridged by Citrix ADC.

sacl6TotPktsDenied

OID: 1.3.6.1.4.1.5951.4.1.1.22.6.2 Packets dropped because they match SimpleACL6 with processing mode set to DENY.

sacl6TotPktsAllowed

OID: 1.3.6.1.4.1.5951.4.1.1.22.6.3 Total packets that matched a SimpleACL6 with action ALLOW and got consumed by Citrix ADC.

sacl6TotHits

OID: 1.3.6.1.4.1.5951.4.1.1.22.6.4 Packets matching a SimpleACL6.

sacl6TotMisses

OID: 1.3.6.1.4.1.5951.4.1.1.22.6.5 Packets not matching any SimpleACL6.

sacl6sCount

OID: 1.3.6.1.4.1.5951.4.1.1.22.6.6 Number of SimpleACL6s configured.

pbr6StatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.22.7 This provides statistical information about the configured PBR6s, in the rs9000 product family of Citrix ADC products.

nsPbr6Table

OID: 1.3.6.1.4.1.5951.4.1.1.22.7.20 This table contains all the PBRs configured This is indexed on the acPbrName .

acPbrName

OID: 1.3.6.1.4.1.5951.4.1.1.22.7.20.1.1 The name of the PBR6

pbr6FullName

OID: 1.3.6.1.4.1.5951.4.1.1.22.7.20.1.2 The full name of the PBR6

pbr6Priority

OID: 1.3.6.1.4.1.5951.4.1.1.22.7.20.1.3 The priority of the PBR6

pbr6perHits

OID: 1.3.6.1.4.1.5951.4.1.1.22.7.20.1.4 Number of times the pbr6 was hit

pbr6TotPktsAllowed

OID: 1.3.6.1.4.1.5951.4.1.1.22.7.21 Total packets that matched the PBR6 with action ALLOW

pbr6TotPktsDenied

OID: 1.3.6.1.4.1.5951.4.1.1.22.7.22 Total packets that matched PBR6 with action DENY

pbr6TotHits

OID: 1.3.6.1.4.1.5951.4.1.1.22.7.23 Total packets that matched one of the configured PBR6

pbr6TotMisses

OID: 1.3.6.1.4.1.5951.4.1.1.22.7.24 Total packets that did not match any PBR6

pbr6TotNullDrop

OID: 1.3.6.1.4.1.5951.4.1.1.22.7.25 Total packets that are dropped due to null next hop

nsHighAvailabilityGroup

OID: 1.3.6.1.4.1.5951.4.1.1.23 This provides information about the High Availability feature in the Netscaler product.

haPeerId

OID: 1.3.6.1.4.1.5951.4.1.1.23.1 The unique identifier to represent the failover peer Citrix ADC

haPeerIpAddress

OID: 1.3.6.1.4.1.5951.4.1.1.23.2 This represents the ipaddress of the failover peer Citrix ADC(Only for HA over IPv4). For HA over IPv6 (as well as IPv4) haPeerInetAddr will contain this information.

haPeerState

OID: 1.3.6.1.4.1.5951.4.1.1.23.3 This represents the state of the failover peer Citrix ADC whether Primary or Secondary

haTotStateTransitions

OID: 1.3.6.1.4.1.5951.4.1.1.23.4 Total number of master state changes that the Citrix ADC has made from primary to secondary and vice-versa.

haTimeofLastStateTransition

OID: 1.3.6.1.4.1.5951.4.1.1.23.5 This represents the time since the Citrix ADC underwent a state change from primary to secondary or vice-versa

haTotStateFail

OID: 1.3.6.1.4.1.5951.4.1.1.23.6 Number of times state changed to PARTIAL_FAIL/ PARTIAL_FAIL_SSL/ROUTEMONITOR_FAIL/COMPLETE_FAIL.

haErrSyncFailure

OID: 1.3.6.1.4.1.5951.4.1.1.23.7 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.

haErrTotNodeDown

OID: 1.3.6.1.4.1.5951.4.1.1.23.8 Total number of heart-beats missed while the peer node was DOWN.

haErrPropMemFail

OID: 1.3.6.1.4.1.5951.4.1.1.23.9 Total number of times memory allocation failed during command propagation.

haErrNsbMemFail

OID: 1.3.6.1.4.1.5951.4.1.1.23.10 Total number of times memory allocation failed while sending heartbeats.

haErrPortSilent

OID: 1.3.6.1.4.1.5951.4.1.1.23.11 Total number of times heartbeat packets were not received on any enabled interface for the duration of the Dead Interval.

haTotTimerRecoveries

OID: 1.3.6.1.4.1.5951.4.1.1.23.12 Total number of times HA engine recovered from tight loops. (i.e., Total number of times HA timers are not called for MAX down time).

haNicsMonitorFailed

OID: 1.3.6.1.4.1.5951.4.1.1.23.14 Interfaces on which HA heartbeats are not being seen

haLastMasterStateTransitionReason

OID: 1.3.6.1.4.1.5951.4.1.1.23.15 The reason for the last master state transition. This gives the conditions under which this node assumed the current state. The current state is available at the oid sysHighAvailabilityMode.0

haPeerSystemState

OID: 1.3.6.1.4.1.5951.4.1.1.23.16 HA peer system state

haErrPropTimeout

OID: 1.3.6.1.4.1.5951.4.1.1.23.17 Number of times propagation timed out.

haCurDerivedInc

OID: 1.3.6.1.4.1.5951.4.1.1.23.18 Derived incarnation based on IOCTLs received.

haCurPeerInc

OID: 1.3.6.1.4.1.5951.4.1.1.23.19 The peer's incarnation as seen from heartbeats.

haErrMasterDispute

OID: 1.3.6.1.4.1.5951.4.1.1.23.20 Number of HA master disputes.

haTotPktTx

OID: 1.3.6.1.4.1.5951.4.1.1.23.21 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.

haTotPktRx

OID: 1.3.6.1.4.1.5951.4.1.1.23.22 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.

haCurStatus

OID: 1.3.6.1.4.1.5951.4.1.1.23.23 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.

haCurState

OID: 1.3.6.1.4.1.5951.4.1.1.23.24 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.

haPeerInetAddrType

OID: 1.3.6.1.4.1.5951.4.1.1.23.25 The address type of haPeerInetAddr

haPeerInetAddr

OID: 1.3.6.1.4.1.5951.4.1.1.23.26 This represents the Internet Address of the failover peer Citrix ADC

haNicMonitorSucceeded

OID: 1.3.6.1.4.1.5951.4.1.1.23.27 Heartbeat succeeded on this nic.

haLastNicMonitorFailed

OID: 1.3.6.1.4.1.5951.4.1.1.23.28 Heartbeat failed on this nic.

vlanTable

OID: 1.3.6.1.4.1.5951.4.1.1.24 The vlan related statistics Table. This is indexed on the vlanId.

vlanId

OID: 1.3.6.1.4.1.5951.4.1.1.24.1.1 This represents the unique id of the vlan

vlanMemberInterfaces

OID: 1.3.6.1.4.1.5951.4.1.1.24.1.2 This represents the list of interfaces on the Citrix ADC that are members of the vlan

vlanTaggedInterfaces

OID: 1.3.6.1.4.1.5951.4.1.1.24.1.3 This represents the list of interfaces on the Citrix ADC that are members of the vlan that carry tagged packets

vlanTotRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.24.1.16 Packets received on the VLAN.

vlanTotRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.24.1.17 Bytes of data received on the VLAN.

vlanTotTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.24.1.18 Packets transmitted on the VLAN.

vlanTotTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.24.1.19 Bytes of data transmitted on the VLAN.

vlanTotDroppedPkts

OID: 1.3.6.1.4.1.5951.4.1.1.24.1.20 Inbound packets dropped by the VLAN upon reception.

vlanTotBroadcastPkts

OID: 1.3.6.1.4.1.5951.4.1.1.24.1.21 Broadcast packets sent and received on the VLAN.

vlanBridgeGroup

OID: 1.3.6.1.4.1.5951.4.1.1.24.1.24 This represents the bridge group to which this vlan is bound.

vlanAliasName

OID: 1.3.6.1.4.1.5951.4.1.1.24.1.25 This is vlan alias name if configured

nsIpAddrTable

OID: 1.3.6.1.4.1.5951.4.1.1.26 This table contains information about the IP addresses configured on the Citrix ADC. This is indexed on the ipAddr.

ipAddr

OID: 1.3.6.1.4.1.5951.4.1.1.26.1.1 This represents an IP address configured on the Citrix ADC

ipNetmask

OID: 1.3.6.1.4.1.5951.4.1.1.26.1.2 This represents the Netmask

ipType

OID: 1.3.6.1.4.1.5951.4.1.1.26.1.3 This represents the IP address type

ipMode

OID: 1.3.6.1.4.1.5951.4.1.1.26.1.4 This represents the IP address mode

ipFreePorts

OID: 1.3.6.1.4.1.5951.4.1.1.26.1.5 This represents the number of unused ports free on this IP

ipVlan

OID: 1.3.6.1.4.1.5951.4.1.1.26.1.6 The vlan to which this ip address is bound.

ipBridgeGroup

OID: 1.3.6.1.4.1.5951.4.1.1.26.1.7 The bridge group to which this ip address is bound.

ipVxlan

OID: 1.3.6.1.4.1.5951.4.1.1.26.1.8 The vxlan to which this ip address is bound.

nsResourceGroup

OID: 1.3.6.1.4.1.5951.4.1.1.41 This provides information about system resources in the Netscaler product.

resCpuUsage

OID: 1.3.6.1.4.1.5951.4.1.1.41.1 CPU utilization percentage.

resMemUsage

OID: 1.3.6.1.4.1.5951.4.1.1.41.2 Percentage of memory utilization on Citrix ADC.

numCPUs

OID: 1.3.6.1.4.1.5951.4.1.1.41.3 The number of active CPUs.

memSizeMB

OID: 1.3.6.1.4.1.5951.4.1.1.41.4 Total amount of system memory, in megabytes.

numSSLCards

OID: 1.3.6.1.4.1.5951.4.1.1.41.5 Number of SSL Cards on the system

nsCPUTable

OID: 1.3.6.1.4.1.5951.4.1.1.41.6 This table contains information about each CPU in Citrix ADC.

This is indexed on the

OID:](#)

nsCPUname

OID: 1.3.6.1.4.1.5951.4.1.1.41.6.1.1 The name of the CPU.

nsCPUusage

OID: 1.3.6.1.4.1.5951.4.1.1.41.6.1.2 CPU utilization percentage.

nsSysHealthTable

OID: 1.3.6.1.4.1.5951.4.1.1.41.7 This table contains information about the System Health status of the Citrix ADC. This is indexed on the sysHealthCounterName.

sysHealthCounterName

OID: 1.3.6.1.4.1.5951.4.1.1.41.7.1.1 This is the health counter name. The counter name is composed with the type of the counter and what it is intended to carry. All voltage counters stats with 'v', fan counters starts with 'fan' and temperature counters starts with 't'. Eg:'v50p' is a voltage counter that carries the value of the +5v counter.

sysHealthCounterValue

OID: 1.3.6.1.4.1.5951.4.1.1.41.7.1.2 The health counters value. The units are 'mv', RPM and degrees Celsius for voltage, fan and temperatures respectively.

nsSysHealthDiskTable

OID: 1.3.6.1.4.1.5951.4.1.1.41.8 This table contains information about the disk space of the Citrix ADC. This is indexed on the sysHealthDiskName.

sysHealthDiskName

OID: 1.3.6.1.4.1.5951.4.1.1.41.8.1.1 The disk name. Disk name always starts with the 'disk' keyword. Eg: disk0, disk1. Currently disk0 is mapped to /flash and disk1 mapped to /var partitions.

sysHealthDiskSize

OID: 1.3.6.1.4.1.5951.4.1.1.41.8.1.2 The total disk space in MBytes (includes available and used spaces also).

sysHealthDiskAvail

OID: 1.3.6.1.4.1.5951.4.1.1.41.8.1.3 The total disk space available in MBytes.

sysHealthDiskUsed

OID: 1.3.6.1.4.1.5951.4.1.1.41.8.1.4 The total disk space used in MBytes.

sysHealthDiskPerusage

OID: 1.3.6.1.4.1.5951.4.1.1.41.8.1.5 The Percentage of the disk space used.

cpuSpeedMHz

OID: 1.3.6.1.4.1.5951.4.1.1.41.15 CPU speed in MHz.

numPEs

OID: 1.3.6.1.4.1.5951.4.1.1.41.16 The Citrix ADC number of PEs running

sysStatisticsTime

OID: 1.3.6.1.4.1.5951.4.1.1.41.17 This gives the timestamp of the statistics returned by SNMP counter values. This can be used for calculating the rate of increments for Counter and Counter64 type of OIDs.

nsIpStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.43 This provides information about IP related statistics in the Netscaler product.

ipTotRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.43.25 IP packets received.

ipTotRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.43.26 Bytes of IP data received.

ipTotRxMbits

OID: 1.3.6.1.4.1.5951.4.1.1.43.27 Megabits of IP data received.

ipTotTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.43.28 IP packets transmitted.

ipTotTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.43.29 Bytes of IP data transmitted.

ipTotTxMbits

OID: 1.3.6.1.4.1.5951.4.1.1.43.30 Megabits of IP data transmitted.

ipTotFragments

OID: 1.3.6.1.4.1.5951.4.1.1.43.31 IP fragments received.

ipTotBadlens

OID: 1.3.6.1.4.1.5951.4.1.1.43.32 Packets received with a length greater than the normal maximum transmission unit of 1514 bytes.

ipTotBadMacAddrs

OID: 1.3.6.1.4.1.5951.4.1.1.43.33 IP packets transmitted with a bad MAC address.

ipTotMaxClients

OID: 1.3.6.1.4.1.5951.4.1.1.43.34 Attempts to open a new connection to a service for which the maximum limit has been exceeded. Default value, 0, applies no limit.

ipTotUnknownSvcs

OID: 1.3.6.1.4.1.5951.4.1.1.43.35 Packets received on a port or service that is not configured.

ipTotLandattacks

OID: 1.3.6.1.4.1.5951.4.1.1.43.36 Land-attack packets received. The source and destination addresses are the same.

ipTotBadChecksums

OID: 1.3.6.1.4.1.5951.4.1.1.43.37 Packets received with an IP checksum error.

ipTotReassemblyAttempt

OID: 1.3.6.1.4.1.5951.4.1.1.43.38 IP packets that the Citrix ADC attempts to reassemble. If one of the fragments is missing, the whole packet is dropped.

ipTotSuccReassembly

OID: 1.3.6.1.4.1.5951.4.1.1.43.39 Fragmented IP packets successfully reassembled on the Citrix ADC.

ipTotUnsuccReassembly

OID: 1.3.6.1.4.1.5951.4.1.1.43.40 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.

ipTotTooBig

OID: 1.3.6.1.4.1.5951.4.1.1.43.41 Packets received for which the reassembled data exceeds the Ethernet packet data length of 1500 bytes.

ipTotZeroFragmentLen

OID: 1.3.6.1.4.1.5951.4.1.1.43.42 Packets received with a fragment length of 0 bytes.

ipTotDupFragments

OID: 1.3.6.1.4.1.5951.4.1.1.43.43 Duplicate IP fragments received. This can occur when the acknowledgement was not received within the expected time.

ipTotOutOfOrderFrag

OID: 1.3.6.1.4.1.5951.4.1.1.43.44 Fragments received that are out of order.

ipTotUnknownDstRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.43.45 Packets received in which the destination IP address was not reachable or not owned by the Citrix ADC.

ipTotBadTransport

OID: 1.3.6.1.4.1.5951.4.1.1.43.46 Packets received in which the protocol specified in the IP header is unknown to the Citrix ADC.

ipTotVIPDown

OID: 1.3.6.1.4.1.5951.4.1.1.43.47 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.

ipTotFixHeaderFail

OID: 1.3.6.1.4.1.5951.4.1.1.43.48 Packets received that contain an error in one or more components of the IP header.

ipTotAddrLookup

OID: 1.3.6.1.4.1.5951.4.1.1.43.49 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.

ipTotAddrLookupFail

OID: 1.3.6.1.4.1.5951.4.1.1.43.50 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.

ipTotUDPfragmentsFwd

OID: 1.3.6.1.4.1.5951.4.1.1.43.51 UDP fragments forwarded to the client or the server.

ipTotTCPfragmentsFwd

OID: 1.3.6.1.4.1.5951.4.1.1.43.52 TCP fragments forwarded to the client or the server.

ipTotFragPktsGen

OID: 1.3.6.1.4.1.5951.4.1.1.43.53 Fragmented packets created by the Citrix ADC.

ipTotInvalidHeaderSz

OID: 1.3.6.1.4.1.5951.4.1.1.43.54 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.

ipTotInvalidPacketSize

OID: 1.3.6.1.4.1.5951.4.1.1.43.55 Total number of packets received by Citrix ADC with invalid IP packet size.

ipTotTruncatedPackets

OID: 1.3.6.1.4.1.5951.4.1.1.43.56 Truncated IP packets received. An overflow in the routers along the path can truncate IP packets.

ipTotZeroNextHop

OID: 1.3.6.1.4.1.5951.4.1.1.43.57 Packets received that contain a 0 value in the next hop field. These packets are dropped.

ipTotTtlExpired

OID: 1.3.6.1.4.1.5951.4.1.1.43.58 Packets for which the time-to-live (TTL) expired during transit. These packets are dropped.

nonIpTotTruncatedPackets

OID: 1.3.6.1.4.1.5951.4.1.1.43.59 Truncated non-IP packets received.

nsIcmpStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.44 This provides information about ICMP related statistics in the Netscaler product.

icmpCurRateThreshold

OID: 1.3.6.1.4.1.5951.4.1.1.44.17 Limit for ICMP packets handled every 10 milliseconds. Default value, 0, applies no limit.This is a configurable value using the set rateControl command.

icmpTotRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.44.22 ICMP packets received.

icmpTotRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.44.23 Bytes of ICMP data received.

icmpTotTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.44.24 ICMP packets transmitted.

icmpTotTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.44.25 Bytes of ICMP data transmitted.

icmpTotRxEchoReply

OID: 1.3.6.1.4.1.5951.4.1.1.44.26 ICMP Ping echo replies received.

icmpTotTxEchoReply

OID: 1.3.6.1.4.1.5951.4.1.1.44.27 ICMP Ping echo replies transmitted.

icmpTotRxEcho

OID: 1.3.6.1.4.1.5951.4.1.1.44.28 ICMP Ping Echo Request and Echo Reply packets received.

icmpTotPktsDropped

OID: 1.3.6.1.4.1.5951.4.1.1.44.29 ICMP packets dropped because the rate threshold has been exceeded.

icmpTotThresholdExceeds

OID: 1.3.6.1.4.1.5951.4.1.1.44.30 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.

icmpTotPortUnreachableRx

OID: 1.3.6.1.4.1.5951.4.1.1.44.31 ICMP Port Unreachable error messages received. This error is generated when there is no service is running on the port.

icmpTotPortUnreachableTx

OID: 1.3.6.1.4.1.5951.4.1.1.44.32 ICMP Port Unreachable error messages generated. This error is generated when there is no service is running on the port.

icmpTotBadChecksum

OID: 1.3.6.1.4.1.5951.4.1.1.44.33 ICMP Fragmentation Needed error messages received with an ICMP checksum error.

icmpTotNeedFragRx

OID: 1.3.6.1.4.1.5951.4.1.1.44.34 ICMP Fragmentation Needed error messages received for packets that need to be fragmented but for which Don't Fragment is specified the header.

icmpTotNonFirstIpFrag

OID: 1.3.6.1.4.1.5951.4.1.1.44.35 ICMP Fragmentation Needed error messages received that were generated by an IP fragment other than the first one.

icmpTotInvalidBodyLen

OID: 1.3.6.1.4.1.5951.4.1.1.44.36 ICMP Fragmentation Needed error messages received that specified an invalid body length.

icmpTotNoTcpConn

OID: 1.3.6.1.4.1.5951.4.1.1.44.37 ICMP Need Fragmentation error messages received for TCP packets. The state of the connection for these packets is not maintained on the Citrix ADC.

icmpTotNoUdpConn

OID: 1.3.6.1.4.1.5951.4.1.1.44.38 ICMP Need Fragmentation error messages received for UDP packets. The state of the connection for these packets is not maintained on the Citrix ADC.

icmpTotInvalidTcpSeqno

OID: 1.3.6.1.4.1.5951.4.1.1.44.39 ICMP Fragmentation Needed error messages received for packets that contain an invalid TCP address.

icmpTotInvalidNextMTUval

OID: 1.3.6.1.4.1.5951.4.1.1.44.40 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.

icmpTotDstIpLookup

OID: 1.3.6.1.4.1.5951.4.1.1.44.41 Total number of MTU lookup on destination IP info received on a need fragmentation ICMP error message failed.

icmpTotBigNextMTU

OID: 1.3.6.1.4.1.5951.4.1.1.44.42 ICMP Fragmentation Needed error messages received in which the value for the next MTU is higher than that of the current MTU.

icmpTotInvalidProtocol

OID: 1.3.6.1.4.1.5951.4.1.1.44.43 ICMP Fragmentation Needed error messages received that contain a protocol other than TCP and UDP.

icmpTotBadPMTUIpChecksum

OID: 1.3.6.1.4.1.5951.4.1.1.44.44 ICMP Fragmentation Needed error messages received with an IP checksum error.

icmpTotPMTUnoLink

OID: 1.3.6.1.4.1.5951.4.1.1.44.45 ICMP Fragmentation Needed error messages received on a Protocol Control Block (PCB) with no link. The PCB maintains the state of the connection.

icmpTotPMTUDiscoveryDisabled

OID: 1.3.6.1.4.1.5951.4.1.1.44.46 ICMP Need Fragmentation error messages received when the PMTU Discovery mode is not enabled.

nsUdpStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.45 This provides information about UDP related statistics in the Netscaler product.

udpCurRateThreshold

OID: 1.3.6.1.4.1.5951.4.1.1.45.11 Limit for UDP packets handled every 10 milliseconds. Default value, 0, applies no limit.This is a configurable value using the set rateControl command.

udpTotUnknownSvcPkts

OID: 1.3.6.1.4.1.5951.4.1.1.45.16 Stray UDP packets dropped due to no configured listening service.

udpTotRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.45.17 Total number of UDP packets received.

udpTotRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.45.18 Total number of UDP data received in bytes.

udpTotTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.45.19 Total number of UDP packets transmitted.

udpTotTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.45.20 Total number of UDP data transmitted in bytes.

udpCurRateThresholdExceeds

OID: 1.3.6.1.4.1.5951.4.1.1.45.21 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.

udpBadChecksum

OID: 1.3.6.1.4.1.5951.4.1.1.45.22 Packets received with a UDP checksum error.

nsTcpStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.46 This provides information about TCP related statistics in the Netscaler product.

tcpCurServerConn

OID: 1.3.6.1.4.1.5951.4.1.1.46.1 Server connections, including connections in the Opening, Established, and Closing state.

tcpCurClientConn

OID: 1.3.6.1.4.1.5951.4.1.1.46.2 Client connections, including connections in the Opening, Established, and Closing state.

tcpActiveServerConn

OID: 1.3.6.1.4.1.5951.4.1.1.46.8 Connections to a server currently responding to requests.

tcpCurClientConnClosing

OID: 1.3.6.1.4.1.5951.4.1.1.46.9 Client connections in the Closing state, which indicates that the connection termination process has initiated but is not complete.

tcpCurServerConnEstablished

OID: 1.3.6.1.4.1.5951.4.1.1.46.10 Current server connections in the Established state, which indicates that data transfer can occur between the Citrix ADC and the server.

tcpCurClientConnOpening

OID: 1.3.6.1.4.1.5951.4.1.1.46.11 Client connections in the Opening state, which indicates that the handshakes are not yet complete.

tcpCurClientConnEstablished

OID: 1.3.6.1.4.1.5951.4.1.1.46.12 Current client connections in the Established state, which indicates that data transfer can occur between the Citrix ADC and the client.

tcpCurServerConnClosing

OID: 1.3.6.1.4.1.5951.4.1.1.46.13 Server connections in the Closing state, which indicates that the connection termination process has initiated but is not complete.

tcpSpareConn

OID: 1.3.6.1.4.1.5951.4.1.1.46.14 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.

tcpSurgeQueueLen

OID: 1.3.6.1.4.1.5951.4.1.1.46.15 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.

tcpCurServerConnOpening

OID: 1.3.6.1.4.1.5951.4.1.1.46.16 Server connections in the Opening state, which indicates that the handshakes are not yet complete.

tcpTotServerConnOpened

OID: 1.3.6.1.4.1.5951.4.1.1.46.17 Server connections initiated by the Citrix ADC since startup. This counter is reset when the Citrix ADC is restarted.

tcpTotServerConnClosed

OID: 1.3.6.1.4.1.5951.4.1.1.46.18 Total number of closed server connections

tcpTotClientConnOpened

OID: 1.3.6.1.4.1.5951.4.1.1.46.19 Client connections opened by the Citrix ADC since startup (after three-way handshake). This counter is reset when the Citrix ADC is restarted.

tcpTotClientConnClosed

OID: 1.3.6.1.4.1.5951.4.1.1.46.20 Total number of closed client connections

tcpTotSyn

OID: 1.3.6.1.4.1.5951.4.1.1.46.21 SYN packets received

tcpTotSynProbe

OID: 1.3.6.1.4.1.5951.4.1.1.46.22 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.

tcpTotSvrFin

OID: 1.3.6.1.4.1.5951.4.1.1.46.23 FIN packets received from the server.

tcpTotCltFin

OID: 1.3.6.1.4.1.5951.4.1.1.46.24 FIN packets received from the clients.

tcpWaitToSyn

OID: 1.3.6.1.4.1.5951.4.1.1.46.25 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.

tcpTotZombieCltConnFlushed

OID: 1.3.6.1.4.1.5951.4.1.1.46.26 Client connections that are flushed because the client has been idle for some time.

tcpTotZombieSvrConnFlushed

OID: 1.3.6.1.4.1.5951.4.1.1.46.27 Server connections that are flushed because there have been no client requests in the queue for some time.

tcpTotZombieHalfOpenCltConnFlushed

OID: 1.3.6.1.4.1.5951.4.1.1.46.28 Half-opened client connections that are flushed because the three-way handshakes are not complete.

tcpTotZombieHalfOpenSvrConnFlushed

OID: 1.3.6.1.4.1.5951.4.1.1.46.29 Half-opened server connections that are flushed because the three-way handshakes are not complete.

tcpTotZombieActiveHalfCloseCltConnFlushed

OID: 1.3.6.1.4.1.5951.4.1.1.46.30 Active half-closed client connections that are flushed because the client has closed the connection and there has been no activity on the connection.

tcpTotZombieActiveHalfCloseSvrConnFlushed

OID: 1.3.6.1.4.1.5951.4.1.1.46.31 Active half-closed server connections that are flushed because the server has closed the connection and there has been no activity on the connection.

tcpTotZombiePassiveHalfCloseCltConnFlushed

OID: 1.3.6.1.4.1.5951.4.1.1.46.32 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.

tcpTotZombiePassiveHalfCloseSrvConnFlushed

OID: 1.3.6.1.4.1.5951.4.1.1.46.33 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.

tcpErrBadCheckSum

OID: 1.3.6.1.4.1.5951.4.1.1.46.34 Packets received with a TCP checksum error.

tcpErrSynInSynRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.46.35 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.

tcpErrSynInEst

OID: 1.3.6.1.4.1.5951.4.1.1.46.36 SYN packets received on a connection that is in the ESTABLISHED state. A SYN packet is not expected on an ESTABLISHED connection.

tcpErrSynGiveUp

OID: 1.3.6.1.4.1.5951.4.1.1.46.37 Attempts to establish a connection on the Citrix ADC that timed out.

tcpErrSynSentBadAck

OID: 1.3.6.1.4.1.5951.4.1.1.46.38 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.

tcpErrSynRetry

OID: 1.3.6.1.4.1.5951.4.1.1.46.39 SYN packets resent to a server.

tcpErrFinRetry

OID: 1.3.6.1.4.1.5951.4.1.1.46.40 FIN packets resent to a server or a client.

tcpErrFinGiveUp

OID: 1.3.6.1.4.1.5951.4.1.1.46.41 Connections that were timed out by the Citrix ADC because of not receiving the ACK packet after retransmitting the FIN packet four times.

tcpErrFinDup

OID: 1.3.6.1.4.1.5951.4.1.1.46.42 Number of duplicate FIN packets recieved

tcpErrRst

OID: 1.3.6.1.4.1.5951.4.1.1.46.43 Reset packets received from a client or a server.

tcpErrRstNonEst

OID: 1.3.6.1.4.1.5951.4.1.1.46.44 Reset packets received on a connection that is not in the ESTABLISHED state.

tcpErrRstOutOfWindow

OID: 1.3.6.1.4.1.5951.4.1.1.46.45 Reset packets received on a connection that is out of the current TCP window.

tcpErrRstInTimewait

OID: 1.3.6.1.4.1.5951.4.1.1.46.46 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.

tcpErrSvrRetrasmit

OID: 1.3.6.1.4.1.5951.4.1.1.46.47 Packets retransmitted by a server. This usually occurs because the acknowledgement from the Citrix ADC has not reached the server.

tcpErrCltRetrasmit

OID: 1.3.6.1.4.1.5951.4.1.1.46.48 Packets retransmitted by a client. This usually occurs because the acknowledgement from the Citrix ADC has not reached the client.

tcpErrFullRetrasmit

OID: 1.3.6.1.4.1.5951.4.1.1.46.49 Full packets retransmitted by the client or the server.

tcpErrPartialRetrasmit

OID: 1.3.6.1.4.1.5951.4.1.1.46.50 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.

tcpErrSvrOutOfOrder

OID: 1.3.6.1.4.1.5951.4.1.1.46.51 Out of order TCP packets received from a server.

tcpErrCltOutOfOrder

OID: 1.3.6.1.4.1.5951.4.1.1.46.52 Out of order TCP packets received from a client.

tcpErrCltHole

OID: 1.3.6.1.4.1.5951.4.1.1.46.53 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.

tcpErrSvrHole

OID: 1.3.6.1.4.1.5951.4.1.1.46.54 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.

tcpErrCookiePktSeqReject

OID: 1.3.6.1.4.1.5951.4.1.1.46.55 SYN cookie packets rejected because they contain an incorrect sequence number.

tcpErrCookiePktSigReject

OID: 1.3.6.1.4.1.5951.4.1.1.46.56 SYN cookie packets rejected because they contain an incorrect signature.

tcpErrCookiePktSeqDrop

OID: 1.3.6.1.4.1.5951.4.1.1.46.57 SYN cookie packets dropped because the sequence number specified in the packets is outside the current window.

tcpErrCookiePktMssReject

OID: 1.3.6.1.4.1.5951.4.1.1.46.58 SYN cookie packets rejected because the maximum segment size (MSS) specified in the packets is incorrect.

tcpErrRetransmit

OID: 1.3.6.1.4.1.5951.4.1.1.46.59 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.

tcpErrRetransmitGiveUp

OID: 1.3.6.1.4.1.5951.4.1.1.46.60 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.

tcpTotRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.46.61 TCP packets received.

tcpTotRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.46.62 Bytes of TCP data received.

tcpTotTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.46.63 TCP packets transmitted.

tcpTotTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.46.64 Bytes of TCP data transmitted.

pcbTotZombieCall

OID: 1.3.6.1.4.1.5951.4.1.1.46.65 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.

tcpTotSynHeld

OID: 1.3.6.1.4.1.5951.4.1.1.46.66 SYN packets held on the Citrix ADC that are waiting for a server connection.

tcpTotSynFlush

OID: 1.3.6.1.4.1.5951.4.1.1.46.67 SYN packets flushed on the Citrix ADC because of no response from the server for three or more seconds.

tcpTotFinWaitClosed

OID: 1.3.6.1.4.1.5951.4.1.1.46.68 Connections closed on the Citrix ADC because the number of connections in the TIME_WAIT state has exceeded the default value of 7000.

tcpErrAnyPortFail

OID: 1.3.6.1.4.1.5951.4.1.1.46.69 Port allocations that have failed on a mapped IP address because the maximum limit of 65536 has been exceeded.

tcpErrIpPortFail

OID: 1.3.6.1.4.1.5951.4.1.1.46.70 Port allocations that have failed on a subnet IP address or vserver IP address because the maximum limit of 65536 has been exceeded.

tcpErrSentRst

OID: 1.3.6.1.4.1.5951.4.1.1.46.71 Reset packets sent to a client or a server.

tcpErrBadStateConn

OID: 1.3.6.1.4.1.5951.4.1.1.46.72 Connections that are not in a valid TCP state.

tcpErrFastRetransmissions

OID: 1.3.6.1.4.1.5951.4.1.1.46.73 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.

tcpErrFirstRetransmissions

OID: 1.3.6.1.4.1.5951.4.1.1.46.74 Packets retransmitted once by the Citrix ADC.

tcpErrSecondRetransmissions

OID: 1.3.6.1.4.1.5951.4.1.1.46.75 Packets retransmitted twice by the Citrix ADC.

tcpErrThirdRetransmissions

OID: 1.3.6.1.4.1.5951.4.1.1.46.76 Packets retransmitted three times by the Citrix ADC.

tcpErrForthRetransmissions

OID: 1.3.6.1.4.1.5951.4.1.1.46.77 Packets retransmitted four times by the Citrix ADC.

tcpErrFifthRetransmissions

OID: 1.3.6.1.4.1.5951.4.1.1.46.78 Packets retransmitted five times by the Citrix ADC.

tcpErrSixthRetransmissions

OID: 1.3.6.1.4.1.5951.4.1.1.46.79 Packets retransmitted six times by the Citrix ADC.

tcpErrSeventhRetransmissions

OID: 1.3.6.1.4.1.5951.4.1.1.46.80 Packets retransmitted seven times by the Citrix ADC. If this fails, the Citrix ADC terminates the connection.

tcpErrDataAfterFin

OID: 1.3.6.1.4.1.5951.4.1.1.46.81 Packets received following a connection termination request. This error is usually caused by a reordering of packets during transmission.

tcpErrRstThreshold

OID: 1.3.6.1.4.1.5951.4.1.1.46.82 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.

tcpErrOutOfWindowPkts

OID: 1.3.6.1.4.1.5951.4.1.1.46.83 Packets received that are out of the current advertised window.

tcpErrSynDroppedCongestion

OID: 1.3.6.1.4.1.5951.4.1.1.46.84 SYN packets dropped because of network congestion.

tcpCurPhysicalServers

OID: 1.3.6.1.4.1.5951.4.1.1.46.85 The number of physical servers that Citrix ADC has open connections with.

tcpReuseHit

OID: 1.3.6.1.4.1.5951.4.1.1.46.86 Total number of client transactions found the server connection in the reuse-pool.

tcpWaitToData

OID: 1.3.6.1.4.1.5951.4.1.1.46.87 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.

tcpErrStrayPkt

OID: 1.3.6.1.4.1.5951.4.1.1.46.88 Number of stray or misrouted packets.

tcpTotClientConnOpenRate

OID: 1.3.6.1.4.1.5951.4.1.1.46.89 Rate at which connections are opened in the system per second.

tcpCurRateThreshold

OID: 1.3.6.1.4.1.5951.4.1.1.46.90 Current threshold for TCP rate control. By default, there is no rate control for TCP.

freeConnHalfClosed

OID: 1.3.6.1.4.1.5951.4.1.1.46.91 Number of half-closed connections that were freed.

freeConnFlushMarked

OID: 1.3.6.1.4.1.5951.4.1.1.46.92 Number of connections freed that were already marked for flush.

freeConnEstd

OID: 1.3.6.1.4.1.5951.4.1.1.46.93 Number of established and active connections freed.

flushThresReached

OID: 1.3.6.1.4.1.5951.4.1.1.46.94 Number of times we reached connection flush threshold.

memFailFlushTrigger

OID: 1.3.6.1.4.1.5951.4.1.1.46.95 Number of flushes triggered through memory failure.

mptcpCurMpcapableSessions

OID: 1.3.6.1.4.1.5951.4.1.1.46.96 The number of current mptcp sessions.

mptcpCurSFConnections

OID: 1.3.6.1.4.1.5951.4.1.1.46.97 The number of current mptcp subflow connections.

mptcpCurPendingJoin

OID: 1.3.6.1.4.1.5951.4.1.1.46.98 The number of current mptcp subflow connections in pending state.

mptcpErrInvalCookie

OID: 1.3.6.1.4.1.5951.4.1.1.46.99 MPTCP invalid cookie received on MP_CAPABLE final ACK.

mptcpErrUnknownToken

OID: 1.3.6.1.4.1.5951.4.1.1.46.100 MPTCP invalid token received on MP_JOIN request.

mptcpErrAddridExist

OID: 1.3.6.1.4.1.5951.4.1.1.46.101 MPTCP MP_JOIN request on existing address id.

mptcpErrMaxSF

OID: 1.3.6.1.4.1.5951.4.1.1.46.102 MPTCP new MP_JOIN request after maximum configured subflows are established.

mptcpErrInvalMAC

OID: 1.3.6.1.4.1.5951.4.1.1.46.103 MPTCP invalid MAC on MP_JOIN final ACK.

mptcpErrBadCksum

OID: 1.3.6.1.4.1.5951.4.1.1.46.104 MPTCP checksum failed. Connection will fallback to regular tcp.

mptcpErrAddrId0

OID: 1.3.6.1.4.1.5951.4.1.1.46.105 MPTCP MP_JOIN request on address id 0.

mptcpErrfastclose

OID: 1.3.6.1.4.1.5951.4.1.1.46.106 MPTCP FAST CLOSE sent.

mptcpErrJoinThreshold

OID: 1.3.6.1.4.1.5951.4.1.1.46.107 MPTCP Global pending MP_JOIN threshold limit is reached, new MP_JOIN request will be dropped sending RST

mptcpErrInvalOpts

OID: 1.3.6.1.4.1.5951.4.1.1.46.108 MPTCP invalid mptcp option is received and is dropped.

mptcpErrInvalRemAddr

OID: 1.3.6.1.4.1.5951.4.1.1.46.109 MPTCP remove address request received on invalid/unknown address id.

mptcpErrVersionNotSupported

OID: 1.3.6.1.4.1.5951.4.1.1.46.110 MPTCP MP_CAPABLE request from unsupported mptcp client.

mptcpErrCryptoNotSupported

OID: 1.3.6.1.4.1.5951.4.1.1.46.111 MPTCP client crypto algorithm not supported.

mptcpErrExtnFlagSet

OID: 1.3.6.1.4.1.5951.4.1.1.46.112 Extension flag is set on MP_CAPABLE request.

mptcpErrResFlagSet

OID: 1.3.6.1.4.1.5951.4.1.1.46.113 MPTCP One or more reserved bits are set on MP_CAPABLE request.

mptcpErrJoinAfterFallback

OID: 1.3.6.1.4.1.5951.4.1.1.46.114 MPTCP New MP_JOIN request received after fallback to regular tcp.

mptcpErrDataFinpassive

OID: 1.3.6.1.4.1.5951.4.1.1.46.115 MPTCP Data FIN received on passive subflow

mptcpErrFastClosepassive

OID: 1.3.6.1.4.1.5951.4.1.1.46.116 MPTCP Fast close received on passive subflow.

mptcpErrFastClose

OID: 1.3.6.1.4.1.5951.4.1.1.46.117 MPTCP FAST_CLOSE received on a subflow.

mptcpErrFastCloseKey

OID: 1.3.6.1.4.1.5951.4.1.1.46.118 MPTCP FAST_CLOSE received with invalid key and the packet is dropped.

mptcpPlainackFallback

OID: 1.3.6.1.4.1.5951.4.1.1.46.119 MPTCP Fallback to regular tcp on receiving plain ACK for DSS.

mptcpPlainackRST

OID: 1.3.6.1.4.1.5951.4.1.1.46.120 MPTCP Sent RST on receiving plain ACK for DSS.

mptcpMPFailSent

OID: 1.3.6.1.4.1.5951.4.1.1.46.121 MPTCP Total MP_FAIL sent due to checksum failure.

mptcpMPFailRecvd

OID: 1.3.6.1.4.1.5951.4.1.1.46.122 MPTCP Total MP_FAIL received and fallback to regular TCP.

mptcpInfiniteMapRecvd

OID: 1.3.6.1.4.1.5951.4.1.1.46.123 MPTCP Received and set infinite map and fallen back to regular TCP.

mptcpTotMpCapSyn

OID: 1.3.6.1.4.1.5951.4.1.1.46.124 MPTCP total MP_CAPABLE received

mptcpTotMpJoinSyn

OID: 1.3.6.1.4.1.5951.4.1.1.46.125 MPTCP total MP_JOIN syn received

mptcpTotMpcapSession

OID: 1.3.6.1.4.1.5951.4.1.1.46.126 MPTCP total sessions created

mptcpTotSFConn

OID: 1.3.6.1.4.1.5951.4.1.1.46.127 MPTCP total Subflow connections created

mptcpTotEstSFReplaced

OID: 1.3.6.1.4.1.5951.4.1.1.46.128 MPTCP Total established subflows replaced due to new MP_JOIN.

mptcpTotPendSFReplaced

OID: 1.3.6.1.4.1.5951.4.1.1.46.129 MPTCP Total pending subflows replaced due to new MP_JOIN.

mptcpCurSessWithoutSFs

OID: 1.3.6.1.4.1.5951.4.1.1.46.130 Current Multipath TCP sessions without any subflows

tcpOptimizationEnabled

OID: 1.3.6.1.4.1.5951.4.1.1.46.131 Total number of connections with TCP optimzation.

tcpOptimizationBypassed

OID: 1.3.6.1.4.1.5951.4.1.1.46.132 Total number of connections that bypassed TCP optimzation.

mptcpTotTxSfFin

OID: 1.3.6.1.4.1.5951.4.1.1.46.133 MPTCP total subflow close requests.

mptcpTotMpcapSteered

OID: 1.3.6.1.4.1.5951.4.1.1.46.134 Total MP_CAPABLE sessions steered

mptcpTotConnEst

OID: 1.3.6.1.4.1.5951.4.1.1.46.135 Total MP_CAPABLE sessions created.

mptcpTotMpcapSynackSent

OID: 1.3.6.1.4.1.5951.4.1.1.46.136 Total number of MP_CAPABLE SYN/ACKs sent.

mptcpTotMpcapFackRecvd

OID: 1.3.6.1.4.1.5951.4.1.1.46.137 Total number of MP_CAPABLE Final ACKs received.

mptcpTotAddrRemoved

OID: 1.3.6.1.4.1.5951.4.1.1.46.138 Total number of addresses removed from MPTCP connection with REMOVE_ADDR option

mptcpTotMpjoinSteered

OID: 1.3.6.1.4.1.5951.4.1.1.46.139 Total MP_JOIN subflows steered

mptcpTotMpjoinSynackSent

OID: 1.3.6.1.4.1.5951.4.1.1.46.140 Total MP_JOIN SYN/ACKs sent.

mptcpTotMpjoinFackRecvd

OID: 1.3.6.1.4.1.5951.4.1.1.46.141 Total number of MP_JOIN Final ACKs

mptcpTotMpjoin4thackSent

OID: 1.3.6.1.4.1.5951.4.1.1.46.142 Total number of Subflow final ACK from peer in 3 way handshake validated with 4th ACK.

mptcpTotFreshAckFrwd

OID: 1.3.6.1.4.1.5951.4.1.1.46.143 Fresh ACK recieved on a subflow

mptcpTotDss

OID: 1.3.6.1.4.1.5951.4.1.1.46.144 Total number of Data Sequence Signal packets.

mptcpTotRxDss

OID: 1.3.6.1.4.1.5951.4.1.1.46.145 MPTCP Total Data Sequence Signal packets received.

mptcpTotTxDSS

OID: 1.3.6.1.4.1.5951.4.1.1.46.146 MMPTCP Total Data Sequence Signal packets sent

mptcpTotDssA

OID: 1.3.6.1.4.1.5951.4.1.1.46.147 Total Data Sequence Signal packets during data transfer with DATA_ACK

mptcpTotDSSa

OID: 1.3.6.1.4.1.5951.4.1.1.46.148 Total Data Sequence Signal packets during data transfer with 8 octet DATA_ACK

mptcpTotDssFreshAck

OID: 1.3.6.1.4.1.5951.4.1.1.46.149 MPTCP total Data Sequence Signal packets during data transfer with fresh ACK

mptcpTotDssM

OID: 1.3.6.1.4.1.5951.4.1.1.46.150 MPTCP total data Sequence Signal packets with Data Sequence Mapping and checksum

mptcpTotDssm

OID: 1.3.6.1.4.1.5951.4.1.1.46.151 MPTCP total data Sequence Signal packets with 8 octet Data Sequence Mapping and checksum

mptcpTotDataLessthanDatalen

OID: 1.3.6.1.4.1.5951.4.1.1.46.152 MPTCP Map amount of data not yet received.

mptcpPrioBackupRx

OID: 1.3.6.1.4.1.5951.4.1.1.46.153 MPTCP Subflow used as backup path.

mptcpPrioClearBackupRx

OID: 1.3.6.1.4.1.5951.4.1.1.46.154 Subflow earlier used only as a backup subflow, changes to regular subflow with MP_PRIO option

mptcpTotInfiniteMapFrwd

OID: 1.3.6.1.4.1.5951.4.1.1.46.155 MPTCP received Data Sequence Signal with infinite map flag (Fallback to regular TCP).

mptcpTotTxDataFin

OID: 1.3.6.1.4.1.5951.4.1.1.46.156 Total MPTCP connection close requests sent

mptcpTotRxDataFin

OID: 1.3.6.1.4.1.5951.4.1.1.46.157 Total MPTCP connection close(DATA_FIN) requests received.

mptcpErrOptionDiscarded

OID: 1.3.6.1.4.1.5951.4.1.1.46.158 Invalid subtype in MPTCP option field and hence discarded.

mptcpErrOptsNoSession

OID: 1.3.6.1.4.1.5951.4.1.1.46.159 MPTCP options sent on non existing connection/subflow PCBs.

mptcpErrRemaddrSelf

OID: 1.3.6.1.4.1.5951.4.1.1.46.160 MPTCP remove address request for self address.

mptcpErrRssfFail

OID: 1.3.6.1.4.1.5951.4.1.1.46.161 Add RSS filter to steer traffic to right node on established MPTCP session failed.

mptcpErrOptsSendRst

OID: 1.3.6.1.4.1.5951.4.1.1.46.162 MPTCP sent RST on receiving improper option field.

mptcpErrNoPayloadlenPkt

OID: 1.3.6.1.4.1.5951.4.1.1.46.163 MPTCP Payload length not specified in packet.

mptcpErrUnsupportedMssNegotiated

OID: 1.3.6.1.4.1.5951.4.1.1.46.164 MPTCP Unsupported MSS negotiated error.

mptcpErrNomapPktRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.46.165 MPTCP Packet received with no Data Sequence Mapping.

mptcpTotMoreDataRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.46.166 MPTCP More data received than the available Data Sequence Mapping.

mptcpErrBadmapConnDrop

OID: 1.3.6.1.4.1.5951.4.1.1.46.167 MPTCP Drop the session incase of invalid Data Sequence map.

mptcpErrDupmapRecvd

OID: 1.3.6.1.4.1.5951.4.1.1.46.168 MPTCP Duplicate maps in Data Sequence map table.

mptcpErrInvalidSfn

OID: 1.3.6.1.4.1.5951.4.1.1.46.169 MPTCP subflow map doesn't exactly match MPTCP session mapping.

mptcpErrMapExists

OID: 1.3.6.1.4.1.5951.4.1.1.46.170 MPTCP sequence map already exists.

mptcpErrRetxPktRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.46.171 Retransmitted Data Recevied on MPTCP session.

mptcpErrSfSessionAllocfail

OID: 1.3.6.1.4.1.5951.4.1.1.46.172 Attaching the subflow to MPTCP session failed due to failure in allocating memory to subflow map table.

mptcpErrMpcapSessionAllocfail

OID: 1.3.6.1.4.1.5951.4.1.1.46.173 Creating a MPTCP connection failed due to failure in allocating memory to MPTCP connection management structure.

mptcpTotMpcapSfpcbAlloc

OID: 1.3.6.1.4.1.5951.4.1.1.46.174 Allocating memory to TCP protocol control block(PCB) for subflow failed.

mptcpTotMpcbAllocfailed

OID: 1.3.6.1.4.1.5951.4.1.1.46.175 Allocating memory to MPTCP protocol control block failed.

mptcpErrNsbAllocFailed

OID: 1.3.6.1.4.1.5951.4.1.1.46.176 Failed to allocate memory to output MPTCP packet.

mptcpErrNosfFreensb

OID: 1.3.6.1.4.1.5951.4.1.1.46.177 MPTCP output a packet without any subflow PCB.

mptcpTotV1MpCapSyn

OID: 1.3.6.1.4.1.5951.4.1.1.46.178 MPTCP total Version1 MP_CAPABLE received

mptcpTotV1MpcapSession

OID: 1.3.6.1.4.1.5951.4.1.1.46.179 MPTCP total V1 sessions created

mptcpCurV1MpcapableSessions

OID: 1.3.6.1.4.1.5951.4.1.1.46.180 The number of current V1 mptcp sessions.

mptcpErrV1DataRecvdPriorToKey

OID: 1.3.6.1.4.1.5951.4.1.1.46.181 MPTCP V1 data received prior to key

nsSslStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.47 This provides information about SSL related statistics in the Netscaler product.

sslCardStatus

OID: 1.3.6.1.4.1.5951.4.1.1.47.1 Status of the SSL card(s). The value should be interpreted in binary form, with each set bit indicates a card as UP.

sslEngineStatus

OID: 1.3.6.1.4.1.5951.4.1.1.47.2 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.

sslSessionsPerSec

OID: 1.3.6.1.4.1.5951.4.1.1.47.3 SSL sessions per second between client and Citrix ADC.

sslTotTransactions

OID: 1.3.6.1.4.1.5951.4.1.1.47.200 Number of SSL transactions on the Citrix ADC

sslTotSSLv3Transactions

OID: 1.3.6.1.4.1.5951.4.1.1.47.202 Total number of SSLv3 transactions on the Citrix ADC.

sslTotTLSv1Transactions

OID: 1.3.6.1.4.1.5951.4.1.1.47.203 Number of TLSv1 transactions on the Citrix ADC.

sslTotSessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.204 Number of SSL sessions on the Citrix ADC.

sslTotSSLv3Sessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.206 Number of SSLv3 sessions on the Citrix ADC.

sslTotTLSv1Sessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.207 Number of TLSv1 sessions on the Citrix ADC.

sslTotExpiredSessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.208 Total number of expired SSL sessions on the Citrix ADC.

sslTotNewSessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.209 Number of new SSL sessions created on the Citrix ADC.

sslTotSessionHits

OID: 1.3.6.1.4.1.5951.4.1.1.47.210 Number of SSL session reuse hits on the Citrix ADC.

sslTotSessionMiss

OID: 1.3.6.1.4.1.5951.4.1.1.47.211 Number of SSL session reuse misses on the Citrix ADC.

sslTotRenegSessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.212 Number of SSL session renegotiations on the Citrix ADC.

sslTotSSLv3RenegSessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.213 Number of session renegotiations done on SSLv3.

sslTotTLSv1RenegSessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.214 Number of SSL session renegotiations done on TLSv1.

sslTotSSLv3Handshakes

OID: 1.3.6.1.4.1.5951.4.1.1.47.216 Number of handshakes on SSLv3 on the Citrix ADC.

sslTotTLSv1Handshakes

OID: 1.3.6.1.4.1.5951.4.1.1.47.217 Number of SSL handshakes on TLSv1 on the Citrix ADC.

sslTotSSLv3ClientAuthentications

OID: 1.3.6.1.4.1.5951.4.1.1.47.219 Number of client authentications done on SSLv3.

sslTotTLSv1ClientAuthentications

OID: 1.3.6.1.4.1.5951.4.1.1.47.220 Number of client authentications done on TLSv1.

sslTotRSA512keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.221 Number of RSA 512-bit key exchanges on the Citrix ADC.

sslTotRSA1024keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.222 Number of RSA 1024-bit key exchanges on the Citrix ADC.

sslTotRSA2048keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.223 Number of RSA 2048-bit key exchanges on the Citrix ADC.

sslTotDH512keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.224 Number of Diffie-Helman 512-bit key exchanges on the Citrix ADC.

sslTotDH1024keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.225 Number of Diffie-Helman 1024-bit key exchanges on the Citrix ADC.

sslTotDH2048keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.226 Number of Diffie-Helman 2048-bit key exchanges on the Citrix ADC.

sslTotRSAAuthorizations

OID: 1.3.6.1.4.1.5951.4.1.1.47.227 Number of RSA authentications on the Citrix ADC.

sslTotDHAuthorizations

OID: 1.3.6.1.4.1.5951.4.1.1.47.228 Number of Diffie-Helman authentications on the Citrix ADC.

sslTotDSSAuthorizations

OID: 1.3.6.1.4.1.5951.4.1.1.47.229 Total number of times DSS authorization is used on the Citrix ADC.

sslTotNULLAuthorizations

OID: 1.3.6.1.4.1.5951.4.1.1.47.230 Number of Null authentications on the Citrix ADC.

sslTot40BitRC4Ciphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.231 Number of RC4 40-bit cipher encryptions on the Citrix ADC.

sslTot56BitRC4Ciphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.232 Number of RC4 56-bit cipher encryptions on the Citrix ADC.

sslTot64BitRC4Ciphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.233 Number of RC4 64-bit cipher encryptions on the Citrix ADC.

sslTot128BitRC4Ciphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.234 Number of RC4 128-bit cipher encryptions on the Citrix ADC.

sslTot40BitDESCiphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.235 Number of DES 40-bit cipher encryptions on the Citrix ADC.

sslTot56BitDESCiphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.236 Number of DES 56-bit cipher encryptions on the Citrix ADC.

sslTot168Bit3DESCiphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.237 Number of DES 168-bit cipher encryptions on the Citrix ADC.

sslTot40BitRC2Ciphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.238 Number of RC2 40-bit cipher encryptions on the Citrix ADC.

sslTot56BitRC2Ciphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.239 Number of RC2 56-bit cipher encryptions on the Citrix ADC.

sslTot128BitRC2Ciphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.240 Number of RC2 128-bit cipher encryptions on the Citrix ADC.

sslTot128BitIDEACiphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.241 Number of IDEA 128-bit cipher encryptions on the Citrix ADC.

sslTotNULLCiphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.242 Number of Null cipher encryptions on the Citrix ADC.

sslTotMD5Mac

OID: 1.3.6.1.4.1.5951.4.1.1.47.243 Number of MD5 hashes on the Citrix ADC.

sslTotSHAMac

OID: 1.3.6.1.4.1.5951.4.1.1.47.244 Number of SHA hashes on the Citrix ADC.

sslTotOffloadBulkDES

OID: 1.3.6.1.4.1.5951.4.1.1.47.245 Number of DES encryptions offloaded to the cryptography card.

sslTotOffloadRSAKeyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.246 Number of RSA key exchanges offloaded to the cryptography card.

sslTotOffloadDHKeyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.247 Number of DH key exchanges offloaded to the cryptography card.

sslTotOffloadSignRSA

OID: 1.3.6.1.4.1.5951.4.1.1.47.248 Number of RSA sign operations offloaded to the cryptography card.

sslBeTotSessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.260 Number of back-end SSL sessions on the Citrix ADC.

sslBeTotSSLv3Sessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.261 Number of back-end SSLv3 sessions on the Citrix ADC.

sslBeTotTLSv1Sessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.262 Number of back-end TLSv1 sessions on the Citrix ADC.

sslBeExpiredSessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.263 Number of back-end export sessions on the Citrix ADC.

sslBeTotSessionMultiplexAttempts

OID: 1.3.6.1.4.1.5951.4.1.1.47.264 Number of back-end SSL session multiplex attempts on the Citrix ADC.

sslBeTotSessionMultiplexAttemptSuccess

OID: 1.3.6.1.4.1.5951.4.1.1.47.265 Number of back-end SSL session multiplex successes on the Citrix ADC.

sslBeTotSessionMultiplexAttemptFails

OID: 1.3.6.1.4.1.5951.4.1.1.47.266 Number of back-end SSL session multiplex failures on the Citrix ADC.

sslBeMaxMultiplexedSessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.267 Number of back-end SSL sessions reused on the Citrix ADC.

sslBeTotSSLv3Handshakes

OID: 1.3.6.1.4.1.5951.4.1.1.47.268 Number of back-end SSLv3 handshakes on the Citrix ADC.

sslBeTotTLSv1Handshakes

OID: 1.3.6.1.4.1.5951.4.1.1.47.269 Number of back-end TLSv1 handshakes on the Citrix ADC.

sslBeTotSSLv3ClientAuthentications

OID: 1.3.6.1.4.1.5951.4.1.1.47.270 Number of back-end SSLv3 client authentications on the Citrix ADC.

sslBeTotTLSv1ClientAuthentications

OID: 1.3.6.1.4.1.5951.4.1.1.47.271 Number of back-end TLSv1 client authentications on the Citrix ADC.

sslBeTotRSA512keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.272 Number of back-end RSA 512-bit key exchanges on the Citrix ADC.

sslBeTotRSA1024keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.273 Number of back-end RSA 1024-bit key exchanges on the Citrix ADC.

sslBeTotRSA2048keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.274 Number of back-end RSA 2048-bit key exchanges on the Citrix ADC.

sslBeTotDH512keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.275 Number of back-end DH 512-bit key exchanges on the Citrix ADC.

sslBeTotDH1024keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.276 Number of back-end DH 1024-bit key exchanges on the Citrix ADC.

sslBeTotDH2048keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.277 Number of back-end DH 2048-bit key exchanges on the Citrix ADC.

sslBeTotRSAAuthorizations

OID: 1.3.6.1.4.1.5951.4.1.1.47.278 Number of back-end RSA authentications on the Citrix ADC.

sslBeTotDHAuthorizations

OID: 1.3.6.1.4.1.5951.4.1.1.47.279 Number of back-end DH authentications on the Citrix ADC.

sslBeTotDSSAuthorizations

OID: 1.3.6.1.4.1.5951.4.1.1.47.280 Number of back-end DSS authentications on the Citrix ADC.

sslBeTotNULLAuthorizations

OID: 1.3.6.1.4.1.5951.4.1.1.47.281 Number of back-end null authentications on the Citrix ADC.

sslBeTot40BitRC4Ciphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.282 Number of back-end RC4 40-bit cipher encryptions on the Citrix ADC.

sslBeTot56BitRC4Ciphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.283 Number of back-end RC4 56-bit cipher encryptions on the Citrix ADC.

sslBeTot64BitRC4Ciphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.284 Number of back-end RC4 64-bit cipher encryptions on the Citrix ADC.

sslBeTot128BitRC4Ciphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.285 Number of back-end RC4 128-bit cipher encryptions on the Citrix ADC.

sslBeTot40BitDESCiphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.286 Number of back-end DES 40-bit cipher encryptions on the Citrix ADC.

sslBeTot56BitDESCiphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.287 Number of back-end DES 56-bit cipher encryptions on the Citrix ADC.

sslBeTot168Bit3DESCiphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.288 Number of back-end 3DES 168-bit cipher encryptions on the Citrix ADC.

sslBeTot40BitRC2Ciphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.289 Number of back-end RC2 40-bit cipher encryptions on the Citrix ADC.

sslBeTot56BitRC2Ciphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.290 Number of back-end RC2 56-bit cipher encryptions on the Citrix ADC.

sslBeTot128BitRC2Ciphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.291 Number of back-end RC2 128-bit cipher encryptions on the Citrix ADC.

sslBeTot128BitIDEACiphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.292 Number of back-end IDEA 128-bit cipher encryptions on the Citrix ADC.

sslBeTotNULLCiphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.293 Number of back-end null cipher encryptions on the Citrix ADC.

sslBeTotMD5Mac

OID: 1.3.6.1.4.1.5951.4.1.1.47.294 Number of back-end MD5 hashes on the Citrix ADC.

sslBeTotSHAMac

OID: 1.3.6.1.4.1.5951.4.1.1.47.295 Number of back-end SHA hashes on the Citrix ADC.

sslCurSessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.296 Number of active SSL sessions on the Citrix ADC.

sslTotOffloadBulkAES

OID: 1.3.6.1.4.1.5951.4.1.1.47.297 Number of AES encryptions offloaded to the cryptography card.

sslTotOffloadBulkRC4

OID: 1.3.6.1.4.1.5951.4.1.1.47.298 Number of RC4 encryptions offloaded to the cryptography card.

sslNumCardsUP

OID: 1.3.6.1.4.1.5951.4.1.1.47.299 Number of SSL cards that are UP. If the number of cards UP is lower than a threshold, a failover is initiated.

sslCards

OID: 1.3.6.1.4.1.5951.4.1.1.47.300 Number of SSL crypto cards present on the Citrix ADC.

sslTotBkendSessionReNegotiate

OID: 1.3.6.1.4.1.5951.4.1.1.47.301 Number of back-end SSL session renegotiations on the Citrix ADC.

sslTotCipherAES128

OID: 1.3.6.1.4.1.5951.4.1.1.47.302 Number of AES 128-bit cipher encryptions on the Citrix ADC.

sslTotBkendSslV3Renego

OID: 1.3.6.1.4.1.5951.4.1.1.47.303 Number of back-end SSLv3 session renegotiations on the Citrix ADC.

sslTotBkendTlSvlRenego

OID: 1.3.6.1.4.1.5951.4.1.1.47.304 Number of back-end TLSv1 session renegotiations on the Citrix ADC.

sslTotCipherAES256

OID: 1.3.6.1.4.1.5951.4.1.1.47.305 Number of AES 256-bit cipher encryptions on the Citrix ADC.

sslTotBkendCipherAES128

OID: 1.3.6.1.4.1.5951.4.1.1.47.306 Back-end AES 128-bit cipher encryptions on the Citrix ADC.

sslTotBkendCipherAES256

OID: 1.3.6.1.4.1.5951.4.1.1.47.307 Back-end AES 256-bit cipher encryptions on the Citrix ADC.

sslTotHwEncBE

OID: 1.3.6.1.4.1.5951.4.1.1.47.308 Number of bytes encrypted in hardware on the back-end.

sslTotDec

OID: 1.3.6.1.4.1.5951.4.1.1.47.309 Number of bytes decrypted on the Citrix ADC.

sslTotSwEncFE

OID: 1.3.6.1.4.1.5951.4.1.1.47.310 Number of bytes encrypted in software on the front-end.

sslTotEncFE

OID: 1.3.6.1.4.1.5951.4.1.1.47.311 Number of bytes encrypted on the front-end.

sslTotEnc

OID: 1.3.6.1.4.1.5951.4.1.1.47.312 Number of bytes encrypted on the Citrix ADC.

sslTotDecHw

OID: 1.3.6.1.4.1.5951.4.1.1.47.313 Number of bytes decrypted in hardware.

sslTotSwDecBE

OID: 1.3.6.1.4.1.5951.4.1.1.47.314 Number of bytes decrypted in software on the back-end

sslTotHwDecFE

OID: 1.3.6.1.4.1.5951.4.1.1.47.315 Number of bytes decrypted in hardware on the front-end.

sslTotEncHw

OID: 1.3.6.1.4.1.5951.4.1.1.47.316 Number of bytes encrypted in hardware.

sslTotDecSw

OID: 1.3.6.1.4.1.5951.4.1.1.47.317 Number of bytes decrypted in software.

sslTotSwEncBE

OID: 1.3.6.1.4.1.5951.4.1.1.47.318 Number of bytes encrypted in software on the back-end.

sslTotEncSw

OID: 1.3.6.1.4.1.5951.4.1.1.47.319 Number of bytes encrypted in software.

sslTotSwDecFE

OID: 1.3.6.1.4.1.5951.4.1.1.47.320 Number of bytes decrypted in software on the front-end.

sslTotEncBE

OID: 1.3.6.1.4.1.5951.4.1.1.47.321 Number of bytes encrypted on the back-end.

sslTotDecBE

OID: 1.3.6.1.4.1.5951.4.1.1.47.322 Number of bytes decrypted on the back-end.

sslTotHwDecBE

OID: 1.3.6.1.4.1.5951.4.1.1.47.323 Number of bytes decrypted in hardware on the back-end.

sslTotDecFE

OID: 1.3.6.1.4.1.5951.4.1.1.47.324 Number of bytes decrypted on the front-end.

sslTotHwEncFE

OID: 1.3.6.1.4.1.5951.4.1.1.47.325 Number of bytes encrypted in hardware on the front-end.

sslTotRSA4096keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.326 Number of RSA 4096-bit key exchanges on the Citrix ADC.

sslCurQSize

OID: 1.3.6.1.4.1.5951.4.1.1.47.327 Current queue size

sslChipReinitCount

OID: 1.3.6.1.4.1.5951.4.1.1.47.328 Count of all reinitialize event for all SSL crypto chips.

sslTotECDHE224keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.329 Number of 224 Elliptical Curve Diffie-Helman on the Citrix ADC.

sslTotECDHE256keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.330 Number of 256 Elliptical Curve Diffie-Helman on the Citrix ADC.

sslTotECDHE384keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.331 Number of 384 Elliptical Curve Diffie-Helman on the Citrix ADC.

sslTotECDHE521keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.332 Number of 521 Elliptical Curve Diffie-Helman on the Citrix ADC.

sslTotTransactionsRate

OID: 1.3.6.1.4.1.5951.4.1.1.47.333 SSL Transactions rate per second.

sslTotSSLv3TransactionsRate

OID: 1.3.6.1.4.1.5951.4.1.1.47.335 SSLv3 Transactions rate per second.

sslTotTLSv1TransactionsRate

OID: 1.3.6.1.4.1.5951.4.1.1.47.336 TLSv1 Transactions rate per second.

sslBeTotEcdheCurve521

OID: 1.3.6.1.4.1.5951.4.1.1.47.337 Number of back-end ECDHE 521 curve Key exchanges on the Citrix ADC.

sslBeTotEcdheCurve384

OID: 1.3.6.1.4.1.5951.4.1.1.47.338 Number of back-end ECDHE 384 curve Key exchanges on the Citrix ADC.

sslBeTotEcdheCurve256

OID: 1.3.6.1.4.1.5951.4.1.1.47.339 Number of back-end ECDHE 256 curve Key exchanges on the Citrix ADC.

sslBeTotEcdheCurve224

OID: 1.3.6.1.4.1.5951.4.1.1.47.340 Number of back-end ECDHE 224 curve Key exchanges on the Citrix ADC.

sslTotTLSv11Handshakes

OID: 1.3.6.1.4.1.5951.4.1.1.47.341 Number of SSL handshakes on TLSv1.1 on the Citrix ADC.

sslTotTLSv12Handshakes

OID: 1.3.6.1.4.1.5951.4.1.1.47.342 Number of SSL handshakes on TLSv1.2 on the Citrix ADC.

sslTotTLSv11Transactions

OID: 1.3.6.1.4.1.5951.4.1.1.47.343 Number of TLSv1.1 transactions on the Citrix ADC.

sslTotTLSv12Transactions

OID: 1.3.6.1.4.1.5951.4.1.1.47.344 Number of TLSv1.2 transactions on the Citrix ADC.

sslTotTLSv11Sessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.345 Number of TLSv1.1 sessions on the Citrix ADC.

sslTotTLSv12Sessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.346 Number of TLSv1.2 sessions on the Citrix ADC.

sslTotTLSv11RenegSessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.347 Number of SSL session renegotiations done on TLSv1.1.

sslTotTLSv12RenegSessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.348 Number of SSL session renegotiations done on TLSv1.2.

sslTotTLSv11ClientAuthentications

OID: 1.3.6.1.4.1.5951.4.1.1.47.349 Number of client authentications done on TLSv1.1.

sslTotTLSv12ClientAuthentications

OID: 1.3.6.1.4.1.5951.4.1.1.47.350 Number of client authentications done on TLSv1.2.

sslTotTLSv11TransactionRate

OID: 1.3.6.1.4.1.5951.4.1.1.47.351 TLSv1.1 Transactions rate per second.

sslTotTLSv12TransactionRate

OID: 1.3.6.1.4.1.5951.4.1.1.47.352 TLSv1.2 Transactions rate per second.

sslTot128BitAESGCMCiphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.353 Number of AEC-GCM 128-bit cipher encryptions on the Citrix ADC.

sslTot256BitAESGCMCiphers

OID: 1.3.6.1.4.1.5951.4.1.1.47.354 Number of AEC-GCM 256-bit cipher encryptions on the Citrix ADC.

sslTotOffloadBulkAESGCM128

OID: 1.3.6.1.4.1.5951.4.1.1.47.355 Number of AES-GCM 128-bit encryptions offloaded to the cryptography card.

sslTotOffloadBulkAESGCM256

OID: 1.3.6.1.4.1.5951.4.1.1.47.356 Number of AES-GCM 256-bit encryptions offloaded to the cryptography card.

sslBeTotTLSv11Sessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.357 Number of back-end TLSv1.1 sessions on the Citrix ADC.

sslBeTotTLSv12Sessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.358 Number of back-end TLSv1.2 sessions on the Citrix ADC.

sslBeTotTLSv11Handshakes

OID: 1.3.6.1.4.1.5951.4.1.1.47.359 Number of back-end TLSv1.1 handshakes on the Citrix ADC.

sslBeTotTLSv12Handshakes

OID: 1.3.6.1.4.1.5951.4.1.1.47.360 Number of back-end TLSv1.2 handshakes on the Citrix ADC.

sslBeTotTLSv11ClientAuthentications

OID: 1.3.6.1.4.1.5951.4.1.1.47.361 Number of back-end TLSv1.1 client authentications on the Citrix ADC.

sslBeTotTLSv12ClientAuthentications

OID: 1.3.6.1.4.1.5951.4.1.1.47.362 Number of back-end TLSv1.2 client authentications on the Citrix ADC.

sslTotBkendTlSv11Renego

OID: 1.3.6.1.4.1.5951.4.1.1.47.363 Number of back-end TLSv1.1 session renegotiations on the Citrix ADC.

sslTotBkendTlSv12Renego

OID: 1.3.6.1.4.1.5951.4.1.1.47.364 Number of back-end TLSv1.2 session renegotiations on the Citrix ADC.

sslCryptoUtilization

OID: 1.3.6.1.4.1.5951.4.1.1.47.365 Utilization of the hardware crypto resource. Only valid values are 0-100%. Only works on platforms with Nitrox-3 chips. A value of 4294967295 is displayed on other platforms.

sslTotECDSAAuthorizations

OID: 1.3.6.1.4.1.5951.4.1.1.47.366 Total number of times ECDSA authorization is used on the Citrix ADC.

sslNumCardsUPSecondary

OID: 1.3.6.1.4.1.5951.4.1.1.47.367 Number of Add on SSL cards that are UP.

sslCardsSecondary

OID: 1.3.6.1.4.1.5951.4.1.1.47.368 Number of secondary SSL crypto cards present on the Citrix ADC.

sslCardStatusSecondary

OID: 1.3.6.1.4.1.5951.4.1.1.47.369 Status of the secondary SSL card(s). The value should be interpreted in binary form, with each set bit indicates a card as UP.

sslCryptoUtilizationSecondary

OID: 1.3.6.1.4.1.5951.4.1.1.47.370 Utilization of the hardware crypto resource. Only valid values are 0-100%. Only works on N3FIPS+N3 hybrid platform. A value of 4294967295 is displayed on other platforms.

sslTotEncHwSecondary

OID: 1.3.6.1.4.1.5951.4.1.1.47.371 Number of bytes encrypted in hardware on secondary card.

sslTotHwEncFEsecondary

OID: 1.3.6.1.4.1.5951.4.1.1.47.372 Number of bytes encrypted on the front-end in hardware on secondary card.

sslTotHwEncBEsecondary

OID: 1.3.6.1.4.1.5951.4.1.1.47.373 Number of bytes encrypted on the back-end in hardware on secondary card.

sslTotDecHwSecondary

OID: 1.3.6.1.4.1.5951.4.1.1.47.374 Number of bytes decrypted in hardware on secondary card.

sslTotHwDecFEsecondary

OID: 1.3.6.1.4.1.5951.4.1.1.47.375 Number of bytes decrypted on the front-end in hardware on secondary card.

sslTotHwDecBEsecondary

OID: 1.3.6.1.4.1.5951.4.1.1.47.376 Number of bytes decrypted on the back-end in hardware on secondary card.

sslBeTotECDSAAuthorizations

OID: 1.3.6.1.4.1.5951.4.1.1.47.377 Number of back-end ECDSA authentications on the Citrix ADC.

sslTotSHA256Mac

OID: 1.3.6.1.4.1.5951.4.1.1.47.378 Number of SHA256 hashes on the Citrix ADC.

sslTotSHA384Mac

OID: 1.3.6.1.4.1.5951.4.1.1.47.379 Number of SHA384 hashes on the Citrix ADC.

sslBeTotSHA256Mac

OID: 1.3.6.1.4.1.5951.4.1.1.47.380 Number of back-end SHA256 hashes on the Citrix ADC.

sslBeTotSHA384Mac

OID: 1.3.6.1.4.1.5951.4.1.1.47.381 Number of back-end SHA384 hashes on the Citrix ADC.

sslTotBkendCipherAESGCM128

OID: 1.3.6.1.4.1.5951.4.1.1.47.382 Back-end AES-GCM 128-bit cipher encryptions on the Citrix ADC.

sslTotBkendCipherAESGCM256

OID: 1.3.6.1.4.1.5951.4.1.1.47.383 Back-end AES-GCM 256-bit cipher encryptions on the Citrix ADC .

sslTotTLSv13Handshakes

OID: 1.3.6.1.4.1.5951.4.1.1.47.384 Number of SSL handshakes on TLSv1.3 on the Citrix ADC.

sslTotTLSv13Transactions

OID: 1.3.6.1.4.1.5951.4.1.1.47.385 Number of TLSv1.3 transactions on the Citrix ADC.

sslTotTLSv13Sessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.386 Number of TLSv1.3 sessions on the Citrix ADC.

sslTotTLSv13ClientAuthentications

OID: 1.3.6.1.4.1.5951.4.1.1.47.387 Number of client authentications done on TLSv1.3.

sslCurTLSv13TransactionRate

OID: 1.3.6.1.4.1.5951.4.1.1.47.388 TLSv1.3 Transactions rate per second.

sslTotDH4096keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.389 Number of Diffie-Helman 4096-bit key exchanges on the Citrix ADC.

sslBeTotRSA4096keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.390 Number of back-end RSA 4096-bit key exchanges on the Citrix ADC.

sslBeTotDH4096keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.391 Number of back-end DH 4096-bit key exchanges on the Citrix ADC.

sslTotDTLSv1Transactions

OID: 1.3.6.1.4.1.5951.4.1.1.47.392 Number of DTLSv1 transactions on the Citrix ADC.

sslTotDTLSv1Sessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.393 Number of DTLSv1 sessions on the Citrix ADC.

sslBeTotDTLSv1Sessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.394 Number of back-end DTLSv1 sessions on the Citrix ADC.

sslTotDTLSv1RenegSessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.395 Number of SSL session renegotiations done on DTLSv1.

sslTotDTLSv1Handshakes

OID: 1.3.6.1.4.1.5951.4.1.1.47.396 Number of SSL handshakes on DTLSv1 on the Citrix ADC.

sslTotDTLSv1ClientAuthentications

OID: 1.3.6.1.4.1.5951.4.1.1.47.397 Number of client authentications done on DTLSv1.

sslTotBkendDTlSvlRenego

OID: 1.3.6.1.4.1.5951.4.1.1.47.398 Number of back-end DTLSv1 session renegotiations on the Citrix ADC.

sslBeTotDTLSv1Handshakes

OID: 1.3.6.1.4.1.5951.4.1.1.47.399 Number of back-end DTLSv1 handshakes on the Citrix ADC.

sslBeTotDTLSv1ClientAuthentications

OID: 1.3.6.1.4.1.5951.4.1.1.47.400 Number of back-end DTLSv1 client authentications on the Citrix ADC.

sslCurDTLSv1TransactionRate

OID: 1.3.6.1.4.1.5951.4.1.1.47.401 DTLSv1 Transactions rate per second.

sslTotRSA3072keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.402 Number of RSA 3072-bit key exchanges on the Citrix ADC.

sslBeTotRSA3072keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.403 Number of back-end RSA 3072-bit key exchanges on the Citrix ADC.

sslCryptoUtilizationAsym

OID: 1.3.6.1.4.1.5951.4.1.1.47.404 Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips. A value of 4294967295 is displayed on other platforms.

sslCryptoUtilizationSymm

OID: 1.3.6.1.4.1.5951.4.1.1.47.405 Utilization of the hardware symmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips. A value of 4294967295 is displayed on other platforms.

sslTotDTLSv12Transactions

OID: 1.3.6.1.4.1.5951.4.1.1.47.406 Number of DTLSv1.2 transactions on the Citrix ADC.

sslTotDTLSv12Sessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.407 Number of DTLSv1.2 sessions on the Citrix ADC.

sslTotDTLSv12RenegSessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.408 Number of SSL session renegotiations done on DTLSv1.2.

sslTotDTLSv12Handshakes

OID: 1.3.6.1.4.1.5951.4.1.1.47.409 Number of SSL handshakes on DTLSv1.2 on the Citrix ADC.

sslTotDTLSv12ClientAuthentications

OID: 1.3.6.1.4.1.5951.4.1.1.47.410 Number of client authentications done on DTLSv1.2.

sslCurDTLSv12TransactionRate

OID: 1.3.6.1.4.1.5951.4.1.1.47.411 DTLSv1.2Transactions rate per second.

sslTotECDHETransactions

OID: 1.3.6.1.4.1.5951.4.1.1.47.412 Total ECDHE Transactions on Citrix ADC.

sslBeTotTLSv13Sessions

OID: 1.3.6.1.4.1.5951.4.1.1.47.413 Number of back-end TLSv1.3 sessions on the Citrix ADC.

sslBeTotTLSv13Handshakes

OID: 1.3.6.1.4.1.5951.4.1.1.47.414 Number of back-end TLSv1.3 handshakes on the Citrix ADC.

sslBeTotTLSv13ClientAuthentications

OID: 1.3.6.1.4.1.5951.4.1.1.47.415 Number of back-end TLSv1.3 client authentications on the Citrix ADC.

sslTotECDHE25519keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.416 Number of 25519 Elliptical Curve Diffie-Helman on the Citrix ADC.

sslAsymCryptoUtilization

OID: 1.3.6.1.4.1.5951.4.1.1.47.417 Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

sslSymCryptoUtilization

OID: 1.3.6.1.4.1.5951.4.1.1.47.418 Utilization of the hardware symmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

sslTotDH3072keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.419 Number of Diffie-Helman 3072-bit key exchanges on the Citrix ADC.

sslBeTotDH3072keyExchanges

OID: 1.3.6.1.4.1.5951.4.1.1.47.420 Number of back-end DH 3072-bit key exchanges on the Citrix ADC.

sslBeTotEcdheCurve25519

OID: 1.3.6.1.4.1.5951.4.1.1.47.421 Number of back-end ECDHE 25519 curve Key exchanges on the Citrix ADC.

nsHttpStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.48 This provides information about HTTP related statistics in the Netscaler product.

httpTotGets

OID: 1.3.6.1.4.1.5951.4.1.1.48.45 Total number of HTTP requests received with the GET method.

httpTotPosts

OID: 1.3.6.1.4.1.5951.4.1.1.48.46 Total number of HTTP requests received with the POST method.

httpTotOthers

OID: 1.3.6.1.4.1.5951.4.1.1.48.47 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.

httpTotRxRequestBytes

OID: 1.3.6.1.4.1.5951.4.1.1.48.48 Total number of bytes of HTTP request data received.

httpTotRxResponseBytes

OID: 1.3.6.1.4.1.5951.4.1.1.48.49 Total number of bytes of HTTP response data received.

httpTotTxRequestBytes

OID: 1.3.6.1.4.1.5951.4.1.1.48.50 Total number of bytes of HTTP request data transmitted.

httpTotTxResponseBytes

OID: 1.3.6.1.4.1.5951.4.1.1.48.51 Total number of bytes of HTTP response data transmitted.

httpTot10Requests

OID: 1.3.6.1.4.1.5951.4.1.1.48.52 Total number of HTTP/1.0 requests received.

httpTotResponses

OID: 1.3.6.1.4.1.5951.4.1.1.48.53 Total number of HTTP responses sent.

httpTot10Responses

OID: 1.3.6.1.4.1.5951.4.1.1.48.54 Total number of HTTP/1.0 responses sent.

httpTotClenResponses

OID: 1.3.6.1.4.1.5951.4.1.1.48.55 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.

httpTotChunkedResponses

OID: 1.3.6.1.4.1.5951.4.1.1.48.56 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.

httpErrIncompleteRequests

OID: 1.3.6.1.4.1.5951.4.1.1.48.57 Total number of HTTP requests received in which the header spans more than one packet.

httpErrIncompleteResponses

OID: 1.3.6.1.4.1.5951.4.1.1.48.58 Total number of HTTP responses received in which the header spans more than one packet.

httpErrIncompleteHeaders

OID: 1.3.6.1.4.1.5951.4.1.1.48.60 Total number of HTTP requests and responses received in which the HTTP header spans more than one packet.

httpErrServerBusy

OID: 1.3.6.1.4.1.5951.4.1.1.48.61 Total number of HTTP error responses received. Some of the error responses are: 500 Internal Server Error501 Not Implemented502 Bad Gateway503 Service Unavailable504 Gateway Timeout505 HTTP Version Not Supported

httpTotChunkedRequests

OID: 1.3.6.1.4.1.5951.4.1.1.48.62 Total number of HTTP requests in which the Transfer-Encoding field of the HTTP header has been set to chunked.

httpTotClenRequests

OID: 1.3.6.1.4.1.5951.4.1.1.48.63 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.

httpErrLargeContent

OID: 1.3.6.1.4.1.5951.4.1.1.48.64 Total number of requests and responses received with large body.

httpErrLargeCtlen

OID: 1.3.6.1.4.1.5951.4.1.1.48.65 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.

httpErrLargeChunk

OID: 1.3.6.1.4.1.5951.4.1.1.48.66 Total number of requests received with large chunk size, in which the Transfer-Encoding field of the HTTP header has been set to chunked.

httpTotRequests

OID: 1.3.6.1.4.1.5951.4.1.1.48.67 Total number of HTTP requests received.

httpTot11Requests

OID: 1.3.6.1.4.1.5951.4.1.1.48.68 Total number of HTTP/1.1 requests received.

httpTot11Responses

OID: 1.3.6.1.4.1.5951.4.1.1.48.69 Total number of HTTP/1.1 responses sent.

httpTotNoClenChunkResponses

OID: 1.3.6.1.4.1.5951.4.1.1.48.70 Total number of FIN-terminated responses sent. In FIN-terminated responses, the server finishes sending the data and closes the connection.

httpErrNoreuseMultipart

OID: 1.3.6.1.4.1.5951.4.1.1.48.71 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.

spdyTotStreams

OID: 1.3.6.1.4.1.5951.4.1.1.48.73 Total number of requests received over SPDYv2 and SPDYv3

spdyv2TotStreams

OID: 1.3.6.1.4.1.5951.4.1.1.48.74 Total number of requests received over SPDYv2

spdyv3TotStreams

OID: 1.3.6.1.4.1.5951.4.1.1.48.75 Total number of requests received over SPDYv3

httpTotRequestsRate

OID: 1.3.6.1.4.1.5951.4.1.1.48.76 Rate at which HTTP Requests are received in the system per second.

httpTotResposesRate

OID: 1.3.6.1.4.1.5951.4.1.1.48.77 Rate at which HTTP Responses are received in the system per second.

httpErrRfc7230DesynCtlenTe

OID: 1.3.6.1.4.1.5951.4.1.1.48.78 Total number of requests/responses received with both content-length and transfer encoding headers - RFC7230 Non-compliance

httpErrRfc7230DesynMultiCtlen

OID: 1.3.6.1.4.1.5951.4.1.1.48.79 Total number of request/response received with multiple content-length headers with different values - RFC7230 Non-compliance

httpErrRfc7230DesynIdenticalCtlen

OID: 1.3.6.1.4.1.5951.4.1.1.48.80 Total number of request/response received with duplicate content-length headers - RFC7230 Non-compliance

httpErrInvalidHostHeader

OID: 1.3.6.1.4.1.5951.4.1.1.48.81 Total number of request received with invalid host header

nsCacheStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.49 This provides information about CACHE related statistics in the Netscaler product.

cacheMaxMemoryKB

OID: 1.3.6.1.4.1.5951.4.1.1.49.1 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.

cacheUtilizedMemoryKB

OID: 1.3.6.1.4.1.5951.4.1.1.49.2 Amount of memory the integrated cache is currently using.

cacheNumCached

OID: 1.3.6.1.4.1.5951.4.1.1.49.3 Responses currently in integrated cache. Includes responses fully downloaded, in the process of being downloaded, and expired or flushed but not yet removed.

cachePercentHit

OID: 1.3.6.1.4.1.5951.4.1.1.49.12 Cache hits as percentage of the total number of requests

cacheRecentPercentHit

OID: 1.3.6.1.4.1.5951.4.1.1.49.13 Recently recorded cache hit ratio expressed as percentage

cacheCurHits

OID: 1.3.6.1.4.1.5951.4.1.1.49.14 This number should be close to the number of hits being served currently.

cacheCurMisses

OID: 1.3.6.1.4.1.5951.4.1.1.49.15 Responses fetched from the origin and served from the cache. Should approximate storable misses. Does not include non-storable misses.

cachePercent304Hits

OID: 1.3.6.1.4.1.5951.4.1.1.49.20 304 responses as a percentage of all responses that the Citrix ADC served.

cacheRecentPercent304Hits

OID: 1.3.6.1.4.1.5951.4.1.1.49.21 Recently recorded ratio of 304 hits to all hits expressed as percentage

cachePercentStoreAbleMiss

OID: 1.3.6.1.4.1.5951.4.1.1.49.26 Responses that were fetched from the origin, stored in the cache, and then served to the client, as a percentage of all cache misses.

cacheRecentPercentStoreAbleMiss

OID: 1.3.6.1.4.1.5951.4.1.1.49.27 Recently recorded ratio of store-able misses to all misses expressed as percentage.

cachePercentSuccessfulRevalidation

OID: 1.3.6.1.4.1.5951.4.1.1.49.34 Percentage of times stored content was successfully revalidated by a 304 (Object Not Modifed) response rather than by a full response

cacheRecentPercentSuccessfulRevalidation

OID: 1.3.6.1.4.1.5951.4.1.1.49.35 Recently recorded percentage of times stored content was successfully revalidated by a 304 response rather than by a full response

cachePercentByteHit

OID: 1.3.6.1.4.1.5951.4.1.1.49.40 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.

cacheRecentPercentByteHit

OID: 1.3.6.1.4.1.5951.4.1.1.49.41 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.

cachePercentOriginBandwidthSaved

OID: 1.3.6.1.4.1.5951.4.1.1.49.42 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.

cacheRecentPercentOriginBandwidthSaved

OID: 1.3.6.1.4.1.5951.4.1.1.49.43 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.

cacheErrMemAlloc

OID: 1.3.6.1.4.1.5951.4.1.1.49.44 Total number of times the cache failed to allocate memory to store responses.

cacheTotRequests

OID: 1.3.6.1.4.1.5951.4.1.1.49.45 Total cache hits plus total cache misses.

cacheTotHits

OID: 1.3.6.1.4.1.5951.4.1.1.49.46 Responses served from the integrated cache. These responses match a policy with a CACHE action.

cacheTotMisses

OID: 1.3.6.1.4.1.5951.4.1.1.49.47 Intercepted HTTP requests requiring fetches from origin server.

cacheTot304Hits

OID: 1.3.6.1.4.1.5951.4.1.1.49.48

Object

OID:not

cacheTotNon304Hits

OID: 1.3.6.1.4.1.5951.4.1.1.49.49 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

cacheTotStoreAbleMisses

OID: 1.3.6.1.4.1.5951.4.1.1.49.50 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.

cacheTotNonStoreAbleMisses

OID: 1.3.6.1.4.1.5951.4.1.1.49.51 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.

cacheTotRevalidationMiss

OID: 1.3.6.1.4.1.5951.4.1.1.49.52 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

cacheTotFullToConditionalRequest

OID: 1.3.6.1.4.1.5951.4.1.1.49.53 Number of user-agent requests for a cached Poll Every Time (PET) response that were sent to the origin server as conditional requests.

cacheTotSuccessfulRevalidation

OID: 1.3.6.1.4.1.5951.4.1.1.49.54 Total number of times stored content was successfully revalidated by a 304 Not Modified response from the origin.

cacheTotResponseBytes

OID: 1.3.6.1.4.1.5951.4.1.1.49.55 Total number of HTTP response bytes served by Citrix ADC from both the origin and the cache

cacheBytesServed

OID: 1.3.6.1.4.1.5951.4.1.1.49.56 Total number of bytes served from the integrated cache

cacheCompressedBytesServed

OID: 1.3.6.1.4.1.5951.4.1.1.49.57 Number of compressed bytes served from the cache

cacheTotPetRequests

OID: 1.3.6.1.4.1.5951.4.1.1.49.58 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).

cacheTotPetHits

OID: 1.3.6.1.4.1.5951.4.1.1.49.59 Number of times a cache hit was found during a search of a content group that has Poll Every Time enabled.

cachePercentPetHits

OID: 1.3.6.1.4.1.5951.4.1.1.49.60 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.

cacheTotParameterizedRequests

OID: 1.3.6.1.4.1.5951.4.1.1.49.61 Total number of requests where the content group has hit and invalidation parameters or selectors.

cacheTotParameterizedHits

OID: 1.3.6.1.4.1.5951.4.1.1.49.62 Parameterized requests resulting in either a 304 or non-304 hit.

cacheTotParameterizedNon304Hits

OID: 1.3.6.1.4.1.5951.4.1.1.49.63 Parameterized requests resulting in a full response (not status code 304: Object Not Updated) served from the cache.

cacheTotParameterized304Hits

OID: 1.3.6.1.4.1.5951.4.1.1.49.64 Parameterized requests resulting in an object not modified (status code 304) response.

cachePercentParameterized304Hits

OID: 1.3.6.1.4.1.5951.4.1.1.49.65 Percentage of parameterized 304 hits relative to all parameterized hits.

cacheRecentPercentParameterizedHits

OID: 1.3.6.1.4.1.5951.4.1.1.49.66 Recently recorded ratio of parameterized 304 hits to all parameterized hits expressed as a percentage

cacheTotInvalidationRequests

OID: 1.3.6.1.4.1.5951.4.1.1.49.67 Requests that match an invalidation policy and result in expiration of specific cached responses or entire content groups.

cacheTotNonParameterizedInvalidationRequests

OID: 1.3.6.1.4.1.5951.4.1.1.49.68 Requests that match an invalidation policy where the invalGroups parameter is configured and expires one or more content groups.

cacheTotParameterizedInvalidationRequests

OID: 1.3.6.1.4.1.5951.4.1.1.49.69 Requests matching a policy with an invalidation (INVAL) action and a content group that uses an invalidation selector or parameters.

cacheLargestResponseReceived

OID: 1.3.6.1.4.1.5951.4.1.1.49.70 Size, in bytes, of largest response sent to client from the cache or the origin server.

cacheTotFlashcacheMisses

OID: 1.3.6.1.4.1.5951.4.1.1.49.71 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.

cacheTotFlashcacheHits

OID: 1.3.6.1.4.1.5951.4.1.1.49.72 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.

cacheTotExpireAtLastByte

OID: 1.3.6.1.4.1.5951.4.1.1.49.73 Instances of content expiring immediately after receiving the last body byte due to the Expire at Last Byte setting for the content group.

cacheNumMarker

OID: 1.3.6.1.4.1.5951.4.1.1.49.74 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.

cacheMaxMemoryActiveKB

OID: 1.3.6.1.4.1.5951.4.1.1.49.75 Currently active value of maximum memory

cache64MaxMemoryKB

OID: 1.3.6.1.4.1.5951.4.1.1.49.76 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.

cacheNumObjSavedOnDisk

OID: 1.3.6.1.4.1.5951.4.1.1.49.77 Cached responses currently saved on disk. Includes responses fully saved to disk, and expired or flushed but not yet removed.

cacheNumMBSavedOnDisk

OID: 1.3.6.1.4.1.5951.4.1.1.49.78 Size (MB) of cached responses currently saved on disk. Includes responses fully saved to disk, and expired or flushed but not yet removed.

cacheNumMBReadFromDisk

OID: 1.3.6.1.4.1.5951.4.1.1.49.79 Total Number of MB read from disk since last reboot.

cacheNumMBWrittenToDisk

OID: 1.3.6.1.4.1.5951.4.1.1.49.80 Total Number of MB written to disk since last reboot.

cacheTotSqlHits

OID: 1.3.6.1.4.1.5951.4.1.1.49.81 sql response served from cache

nsCompressionStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.50 This provides information about Compression related statistics in the Netscaler product.

compTotalRequests

OID: 1.3.6.1.4.1.5951.4.1.1.50.1 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.

compTotalTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.50.2 Number of bytes the Citrix ADC sends to the client after compressing the response from the server.

compTotalRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.50.3 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.

compTotalTxPackets

OID: 1.3.6.1.4.1.5951.4.1.1.50.4 Number of HTTP packets that the Citrix ADC sends to the client after compressing the response from the server.

compTotalRxPackets

OID: 1.3.6.1.4.1.5951.4.1.1.50.5 Number of HTTP packets that can be compressed, which the Citrix ADC receives from the server.

compRatio

OID: 1.3.6.1.4.1.5951.4.1.1.50.6 Ratio of compressible data received to compressed data transmitted expressed as percentage.

compTotalDataCompressionRatio

OID: 1.3.6.1.4.1.5951.4.1.1.50.7 Ratio of total HTTP data received to total HTTP data transmitted expressed as percentage.

compTcpTotalTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.50.8 Number of bytes that the Citrix ADC sends to the client after compressing the response from the server.

compTcpTotalRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.50.9 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.

compTcpTotalTxPackets

OID: 1.3.6.1.4.1.5951.4.1.1.50.10 Number of TCP packets that the Citrix ADC sends to the client after compressing the response from the server.

compTcpTotalRxPackets

OID: 1.3.6.1.4.1.5951.4.1.1.50.11 Total number of compressible packets received by Citrix ADC.

compTcpTotalQuantum

OID: 1.3.6.1.4.1.5951.4.1.1.50.12 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.

compTcpTotalPush

OID: 1.3.6.1.4.1.5951.4.1.1.50.13 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.

compTcpTotalEoi

OID: 1.3.6.1.4.1.5951.4.1.1.50.14 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.

compTcpTotalTimer

OID: 1.3.6.1.4.1.5951.4.1.1.50.15 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.

compTcpRatio

OID: 1.3.6.1.4.1.5951.4.1.1.50.16 Ratio of compressible data received to compressed data transmitted expressed as percentage.

compTcpBandwidthSaving

OID: 1.3.6.1.4.1.5951.4.1.1.50.17 Bandwidth saving from TCP compression expressed as percentage.

deCompTcpRxPackets

OID: 1.3.6.1.4.1.5951.4.1.1.50.18 Total number of compressed packets received by Citrix ADC.

deCompTcpTxPackets

OID: 1.3.6.1.4.1.5951.4.1.1.50.19 Total number of decompressed packets transmitted by Citrix ADC.

deCompTcpRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.50.20 Total number of compressed bytes received by Citrix ADC.

deCompTcpTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.50.21 Total number of decompressed bytes transmitted by Citrix ADC.

deCompTcpErrData

OID: 1.3.6.1.4.1.5951.4.1.1.50.22 Number of data errors encountered while decompressing.

deCompTcpErrLessData

OID: 1.3.6.1.4.1.5951.4.1.1.50.23 Number of times Citrix ADC received less data than declared by protocol.

deCompTcpErrMoreData

OID: 1.3.6.1.4.1.5951.4.1.1.50.24 Number of times Citrix ADC received more data than declared by protocol.

deCompTcpErrMemory

OID: 1.3.6.1.4.1.5951.4.1.1.50.25 Number of times memory failures occurred while decompressing.

deCompTcpErrUnknown

OID: 1.3.6.1.4.1.5951.4.1.1.50.26 Number of times unknown errors occurred while decompressing.

deCompTcpRatio

OID: 1.3.6.1.4.1.5951.4.1.1.50.27 Ratio of decompressed data transmitted to compressed data received expressed as percentage.

deCompTcpBandwidthSaving

OID: 1.3.6.1.4.1.5951.4.1.1.50.28 Bandwidth saving from compression expressed as percentage.

delCompTotalRequests

OID: 1.3.6.1.4.1.5951.4.1.1.50.29 Total number of delta compression requests received by Citrix ADC.

delCompFirstAccess

OID: 1.3.6.1.4.1.5951.4.1.1.50.30 Total number of delta compression first accesses.

delCompDone

OID: 1.3.6.1.4.1.5951.4.1.1.50.31 Total number of delta compressions done by Citrix ADC.

delCompTcpRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.50.32 Total number of delta-compressible bytes received by Citrix ADC.

delCompTcpTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.50.33 Total number of delta-compressed bytes transmitted by Citrix ADC.

delCompTcpRxPackets

OID: 1.3.6.1.4.1.5951.4.1.1.50.34 Number of delta-compressible packets received.

delCompTcpTxPackets

OID: 1.3.6.1.4.1.5951.4.1.1.50.35 Total number of delta-compressed packets transmitted by Citrix ADC.

delCompBaseServed

OID: 1.3.6.1.4.1.5951.4.1.1.50.36 Total number of basefile requests served by Citrix ADC.

delCompBaseTcpTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.50.37 Number of basefile bytes transmitted by Citrix ADC.

delCompErrBypassed

OID: 1.3.6.1.4.1.5951.4.1.1.50.39 Number of times delta-compression bypassed by Citrix ADC.

delCompErrBFileWHdrFailed

OID: 1.3.6.1.4.1.5951.4.1.1.50.40 Number of times basefile could not be updated in Citrix ADC cache.

delCompErrNostoreMiss

OID: 1.3.6.1.4.1.5951.4.1.1.50.41 Number of times basefile was not found in Citrix ADC cache.

delCompErrReqinfoToobig

OID: 1.3.6.1.4.1.5951.4.1.1.50.42 Number of times basefile request URL was too large.

delCompErrReqinfoAllocfail

OID: 1.3.6.1.4.1.5951.4.1.1.50.43 Number of times requested basefile could not be allocated.

delCompErrSessallocFail

OID: 1.3.6.1.4.1.5951.4.1.1.50.44 Number of times delta compression session could not be allocated.

delCmpRatio

OID: 1.3.6.1.4.1.5951.4.1.1.50.45 Ratio of compressible data received to compressed data transmitted expressed as percentage.

delBwSaving

OID: 1.3.6.1.4.1.5951.4.1.1.50.46 Bandwidth saving from delta compression expressed as percentage.

compHttpBandwidthSaving

OID: 1.3.6.1.4.1.5951.4.1.1.50.47 Bandwidth saving from TCP compression expressed as percentage.

gslbGlobalStats

OID: 1.3.6.1.4.1.5951.4.1.1.51.1 This provides information about GSLB related statistics in the Netscaler product.

customEntries

OID: 1.3.6.1.4.1.5951.4.1.1.51.1.1 This is the number of custom locations

staticEntries

OID: 1.3.6.1.4.1.5951.4.1.1.51.1.2 This is the number of static locations

gslbSitesTable

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1 This table contains gslb sites information This is indexed on the siteName.

siteName

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.1 This is the name of the gslb site

siteIp

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.2 The private IP address of this GSLB site.

siteType

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.3 Indicates whether this GSLB site is local or remote.

siteMetricExchange

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.4 Indicates whether metric exchange is enabled or disabled at this GSLB site.

sitePublicIp

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.6 The public IP address of this GSLB site.

siteTotalRequests

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.7 Total number of requests received by the virtual servers represented by all GSLB services associated with this GSLB site.

siteTotalRequestBytes

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.8 Total number of request bytes received by the virtual servers represented by all GSLB services associated with this GSLB site.

siteTotalResponses

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.9 Number of responses received by the virtual servers represented by all GSLB services associated with this GSLB site.

siteTotalResponseBytes

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.10 Number of response bytes received by the virtual servers represented by all GSLB services associated with this GSLB site.

siteCurSrvrConnections

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.11 Number of current connections to the real servers behind the virtual servers represented by all GSLB services associated with this GSLB site.

siteCurClntConnections

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.12 Number of current client connections to the virtual servers represented by all GSLB services associated with this GSLB site.

siteMetricMepStatus

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.13 Indicates the status of the site metric Metric Exchange connection at this GSLB site.

nwMetricMepStatus

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.14 Indicates the status of the network metric Metric Exchange connection at this GSLB site.

nwMetricExchange

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.15 Indicates whether network metric exchange is enabled or disabled at this GSLB site.

persExchange

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.16 Indicates whether Persistence entries exchange is enabled or disabled at this GSLB site.

gslbSiteInetAddressType

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.17 The address type of gslbSiteInetAddress

gslbSiteInetAddress

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.18 The internet address of the gslb site.

gslbSitePublicInetAddressType

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.19 The address type of gslbSitePublicInetAddress

gslbSitePublicInetAddress

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.20 The internet address of the gslb site public IP.

gslbSiteRsyncState

OID: 1.3.6.1.4.1.5951.4.1.1.51.2.1.1.21 State of RSYNC port on the remote site

nsDomainTable

OID: 1.3.6.1.4.1.5951.4.1.1.51.3.1 This table contains information about the Hits on the Domains. This is indexed on the domainName .

domainName

OID: 1.3.6.1.4.1.5951.4.1.1.51.3.1.1.1 The domain name

dnsTotalQueries

OID: 1.3.6.1.4.1.5951.4.1.1.51.3.1.1.2 Total number of DNS queries received.

domainNameFull

OID: 1.3.6.1.4.1.5951.4.1.1.51.3.1.1.3 Full Domain name string

nsPolicyStatsTable

OID: 1.3.6.1.4.1.5951.4.1.1.52.1 This table contains the statistics for all policies This is indexed on the pengPolicyName.

pengPolicyName

OID: 1.3.6.1.4.1.5951.4.1.1.52.1.1.1 Encoded name of the policy

pengPolicyHits

OID: 1.3.6.1.4.1.5951.4.1.1.52.1.1.2 Total policy hits count

pengBytesIn

OID: 1.3.6.1.4.1.5951.4.1.1.52.1.1.3 Input traffic of a compression policy

pengBytesOut

OID: 1.3.6.1.4.1.5951.4.1.1.52.1.1.4 Output traffic of a compression policy

pengPolicyFullName

OID: 1.3.6.1.4.1.5951.4.1.1.52.1.1.5 Full name of the policy

nsDnsServerStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.53.1 This provides information about Domain Name Service related statistics in the Netscaler product.

dnsTotQueries

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.1 Total number of DNS queries received.

dnsTotAnswers

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.2 Total number of DNS responses received.

dnsTotUnsupportedResponseClass

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.13 Total number of responses for which response types were unsupported.

dnsTotUnsupportedResponseType

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.14 Total number of responses for which response type requested was unsupported.

dnsTotUnsupportedQueries

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.15 Total number of requests for which query type requested was unsupported.

dnsTotUnsupportedQueryClass

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.16 Total number of queries for which query class was unsupported.

dnsTotInvalidQueryFormat

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.17 Total number of queries whose format was invalid.

dnsTotNonAuthNoDatas

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.18 Total number of responses for which there was a format error.

dnsTotMultiQuery

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.19 Total number of Multi Query request received.

dnsTotStrayAnswer

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.20 Total number of stray answers.

dnsTotCacheFlush

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.21 Total number of times cache was flushed.

dnsTotCacheEntriesFlush

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.22 Total number of cache entries flushed.

dnsTotServerQuery

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.23 Total number of Server queries sent.

dnsTotServerResponse

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.24 Total number of Server responses received.

dnsTotRecUpdate

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.34 Total number of record updates.

dnsTotMultiQueryDisableError

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.35 Total number of times a multi query was disabled and received a multi query.

dnsCurAuthEntries

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.41 Total number of authoritative entries.

dnsCurNoAuthEntries

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.42 Total number of non-authoritative entries.

dnsTotAuthAns

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.43 Number of queries which were authoritatively answered.

dnsTotAuthNoNames

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.44 Number of queries for which no record was found.

dnsTotNoDataResps

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.45 Number of DNS responses received without answer.

dnsTotResponseBadLen

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.46 Number of DNS responses received with invalid resoure data length.

dnsTotReqRefusals

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.47 Number of DNS requests refused.

dnsTotOtherErrors

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.48 Total number of other errors.

dns64TotQueries

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.68 Total number of DNS64 queries recieved.

dns64TotAnswers

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.69 Total number of DNS64 answers served.

dns64TotsvrAQueries

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.70 Total number of Queries sent by DNS64 module to backend.

dnsErrNullAttack

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.71 Total number of queries received where all the counts are 0.

dnsTotJumboQueries

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.72 Total number of Jumbo DNS queries received over UDP.

dnsTotJumboAnswers

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.73 Total number of Jumbo DNS responses sent over UDP.

dnsTotJumboServerResponses

OID: 1.3.6.1.4.1.5951.4.1.1.53.1.74 Total number of Jumbo DNS responses received over UDP.

nsdnsRegisterTable

OID: 1.3.6.1.4.1.5951.4.1.1.53.2 This table contains statistics about each DNS record type This is indexed on the dnsRecordType .

dnsRecordType

OID: 1.3.6.1.4.1.5951.4.1.1.53.2.1.1 DNS record type

dnsTotEntries

OID: 1.3.6.1.4.1.5951.4.1.1.53.2.1.2 Total number of DNS record entries

dnsTotUpdates

OID: 1.3.6.1.4.1.5951.4.1.1.53.2.1.3 Total number of DNS proactive updates

dnsTotResponses

OID: 1.3.6.1.4.1.5951.4.1.1.53.2.1.4 Total number of DNS server responses

dnsTotRequests

OID: 1.3.6.1.4.1.5951.4.1.1.53.2.1.5 Total number of DNS queries recieved

dnsTotErrLimits

OID: 1.3.6.1.4.1.5951.4.1.1.53.2.1.6 Total number of times we have recieved dns record with more entries than we support

dnsTotErrRespForm

OID: 1.3.6.1.4.1.5951.4.1.1.53.2.1.7 Total number of times we have recieved malformed responses from the backend

dnsTotErrAliasEx

OID: 1.3.6.1.4.1.5951.4.1.1.53.2.1.8 Total number of times we have recieved non-cname record for a domain for which an alias exists

dnsTotErrNoDomains

OID: 1.3.6.1.4.1.5951.4.1.1.53.2.1.9 Total number of cache misses

dnsCurEntries

OID: 1.3.6.1.4.1.5951.4.1.1.53.2.1.10 Current number of DNS entries

dnsCurRecords

OID: 1.3.6.1.4.1.5951.4.1.1.53.2.1.11 Current number of DNS Records

dnsTotQueryForExpiredRecord

OID: 1.3.6.1.4.1.5951.4.1.1.53.2.1.12 Total number of times query was received for expired record

nsIfStatsTable

OID: 1.3.6.1.4.1.5951.4.1.1.54 The interface related statistics Table. This is indexed on the ifName.

ifName

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.1 The name of the interface.

ifMedia

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.2 The media type of the interface.

ifTotRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.3 Number of bytes received by an interface since the Citrix ADC was started or the interface statistics were cleared.

ifRxAvgBandwidthUsage

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.4 The average bandwidth, in bits per second, at which the specified interface has been receiving packets since the Citrix ADC was started or the interface statistics were cleared.

ifTotRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.5 Number of packets received by an interface since the Citrix ADC was started or the interface statistics were cleared.

ifRxAvgPacketRate

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.6 Average rate, in packets per second, of incoming packets on the specified interface since the Citrix ADC was started or the interface statistics were cleared.

ifTotTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.7 Number of bytes transmitted by an interface since the Citrix ADC was started or the interface statistics were cleared.

ifTxAvgBandwidthUsage

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.8 The average bandwidth, in bits per second, at which the specified interface has been transmitting packets since the Citrix ADC was started or the interface statistics were cleared.

ifTotTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.9 Number of packets transmitted by an interface since the Citrix ADC was started or the interface statistics were cleared.

ifTxAvgPacketRate

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.10 Average rate, in packets per second, of outgoing packets on the specified interface since the Citrix ADC was started or the interface statistics were cleared.

ifRxCRCErrors

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.11 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.

ifRxFrameErrors

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.12 Number of Jumbo frames(frame size greater than 1518 bytes) received by the specified interface since the Citrix ADC was started or the interface statistics were cleared.

ifRxAlignmentErrors

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.13 Number of packets received with an alignment error (an error that occurs when the total number of bits of a received frame is not divisible by eight) by the specified interface. Since the Citrix ADC was started or the interface statistics were cleared.

ifTxCarrierError

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.18 Number of Carrier Sense errors that occur when an interface attempts to transmit a frame but is unable to do so as no carrier is detected. This statistic is applicable only to half-duplex transmissions and is available only on 1G data ports of the Citrix ADC 12000 platform and management ports of Citrix ADC MPX 15000 and 17000 platforms. (1) Loop back interface (LO) of all platforms indicates PE fails to send packets to BSD stack because of lack of resources in BSD stack. (2) Number of non Cisco Heart beat packet drop on internal interface. Applicable for internal interface(which is used to communicate between NXOS-NSVSB) of VPX's running on Cisco Nexus platform

ifTotRxMbits

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.19 The total data, in megabits, received by an interface since the Citrix ADC was started or the interface statistics were cleared. This statistic also includes the Ethernet overhead bytes, i.e. preamble, inter-packet gap, and CRC.

ifTotTxMbits

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.20 The total data, in megabits, transmitted by an interface since the Citrix ADC was started or the interface statistics were cleared. This statistic also includes the Ethernet overhead bytes, i.e. preamble, inter-packet gap, and CRC.

ifTotCitrix ADCPkts

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.21 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.

ifErrDroppedRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.22 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.

ifErrLinkHangs

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.23 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.

ifLinkReinits

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.24 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.

ifErrCongestedPktsDrops

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.26 Number of outbound packets dropped from the normal and low-priority transmit (Tx) overflow queues, during congestion on the specified interface, since the Citrix ADC was started or the interface statistics were cleared. This could be caused by one of the following: 1) Packets that have been in the overflow queue for more than 10 milliseconds. 2) Shortage of free receive buffers on the Citrix ADC.

ifErrCongestionLimitPktDrops

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.27 Number of transmit (Tx) packets dropped from normal and low-priority transmit overflow queues, during congestion on the specified interface, since the Citrix ADC was started or the interface statistics were cleared. This is caused when the overflow queue limits are exceeded.

ifErrPktRx

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.28 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.

ifErrRxFIFO

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.29 Number packet drops due to insufficient space in the receive queue, on the specified interface, since the Citrix ADC was started or the interface statistics were cleared. This statistic is only available on the data ports of the Citrix ADC 12000 platform and the Citrix ADC MPX 15000 and 17000 platforms.

ifErrRxNoBuffs

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.30 Number of times the NIC hardware reported an error, due to packets drops caused by lack of buffers. This statistic is available on: (1) All ports except management ports on Citrix ADC MPX 15000 and 17000 platforms. (2) All 1G ports on Citrix ADC MPX 7500, 9500, 10500, 12500, 15500, 17500, 19500, and 21500 platforms.

ifErrRxFCS

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.32 Number of packets received with Frame Check Sequence(FCS) errors, on the specified interface, since the Citrix ADC was started or the interface statistics were cleared. This statistic is available only on data ports of the Citrix ADC 12000 platform and Citrix ADC MPX 15000 and 17000 platforms.

ifErrPktTx

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.33 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.

ifErrTxFIFO

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.34 Number of times the hardware reported an error in accumulating packets for transmission on the specified interface. This statistic is only available on 10G ports of the Citrix ADC 12000-10G platform and data ports of the Citrix ADC MPX 15000 and 17000 platforms. (1) Loop back interfaces (LO) of all platform indicates packets crossed allowed limit, which is 10K PPS on LO interface

ifErrTxHeartBeat

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.35

Number

OID:of

ifErrTxOverflow

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.36 Number of packets that have passed through the overflow queues, during transmission on the specified interface, since the Citrix ADC was started or the interface statistics were cleared. This gets incremented only on congested ports.

ifErrDroppedTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.38 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.

ifTotRxXonPause

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.39 Number of Pause frames received on the specified interface with pause time set to zero. This statistic is not available on 10G ports of the Citrix ADC 12000-10G platform and data ports of the Citrix ADC MPX 15000 and 17000 platforms.

ifTotRxXoffPause

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.40 Number of Pause frames received by the specified interface with the pause time greater than zero. This statistic is only available on 10G ports of the Citrix ADC 12000-10G platform and data ports of the Citrix ADC MPX 15000 and 17000 platforms.

ifTotXoffStateEntered

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.41 Number of times transmission was stopped on the specified interface due to the receipt of Pause frames. This statistic is only available on 10G ports of the Citrix ADC 12000-10G platform and data ports of the Citrix ADC MPX 15000 and 17000 platforms.

ifTotXonSent

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.42 Number of pause frames, sent by the specified interface, with pause time set to zero to restart transmission. This statistic is not available on 10G ports of the Citrix ADC 12000-10G platform and data ports of the Citrix ADC MPX 15000 and 17000 platforms.

ifTotXoffSent

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.43 Number of Pause frames sent by the specified interface with the pause time greater than zero. This statistic is only available on 10G ports of the Citrix ADC 12000-10G platform and data ports of the Citrix ADC MPX 15000 and 17000 platforms. This statistic also includes the Pause frames with pause time equal to zero.

ifnicStsStalls

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.44 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.

ifnicTxStalls

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.45 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.

ifnicRxStalls

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.46 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.

ifnicErrDisables

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.47 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.

ifThroughput

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.48 Interface throughput in Mbps

ifMinThroughput

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.49 Interface minimum throughput in Mbps

ifErrDroppedRxPktsRl

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.50 Number of packets dropped due to license limit on the specified interface.

ifErrRxNoNSB

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.51 Number of times the Citrix ADC failed to allocate buffers, for inbound packets, for the specified interface since the Citrix ADC was started or the interface statistics were cleared.

ifInterfaceAlias

OID: 1.3.6.1.4.1.5951.4.1.1.54.1.52 Alias Name for the Interface

scPolicyStatistics

OID: 1.3.6.1.4.1.5951.4.1.1.55.1 This provides information about Sure Connect Policy related statistics in the Netscaler product.

scPolicyUrlHits

OID: 1.3.6.1.4.1.5951.4.1.1.55.1.1 Total number of incoming requests that matched configured sureconnect policies.

scPopUps

OID: 1.3.6.1.4.1.5951.4.1.1.55.1.2 Total number of in-memory java script served which throws the pop-up window.

scAltContUrls

OID: 1.3.6.1.4.1.5951.4.1.1.55.1.3 Total number of alternate content served which throws the pop-up window.

scSessionReqs

OID: 1.3.6.1.4.1.5951.4.1.1.55.1.4 Total number of requests that were handled in a single SureConnect session.

scPostReqs

OID: 1.3.6.1.4.1.5951.4.1.1.55.1.5 Total number of HTTP POST requests that triggered SureConnect feature.

scThresholdFail

OID: 1.3.6.1.4.1.5951.4.1.1.55.1.6 Total number of times SureConnect was not triggered because the thresholds conditions failed.

scFaultyCookies

OID: 1.3.6.1.4.1.5951.4.1.1.55.1.7 Total number of corrupted SureConnect cookies.

scUnSupBrow

OID: 1.3.6.1.4.1.5951.4.1.1.55.1.8 Total number of requests that came from all unsupported browsers.

scResetStats

OID: 1.3.6.1.4.1.5951.4.1.1.55.1.9 Toal number of times that SureConnect statistics were reset.

scTotCondTriggered

OID: 1.3.6.1.4.1.5951.4.1.1.55.1.10 Number of times that SureConnect conditions were triggered.

scTotReissuedRequests

OID: 1.3.6.1.4.1.5951.4.1.1.55.1.11 Total number of reissued SureConnect requests.

scPolicyConfigTable

OID: 1.3.6.1.4.1.5951.4.1.1.55.2.1 The sure connect policy configuration table This is indexed on the scPolicyName .

scPolicyName

OID: 1.3.6.1.4.1.5951.4.1.1.55.2.1.1.1 The name of Sure Connect policy.

scPolUrl

OID: 1.3.6.1.4.1.5951.4.1.1.55.2.1.1.2 The URL in the IOH Policy.

scDelayThreshold

OID: 1.3.6.1.4.1.5951.4.1.1.55.2.1.1.3 The delay threshold for sc policy.

scMaxConnections

OID: 1.3.6.1.4.1.5951.4.1.1.55.2.1.1.4 The max connections for sc policy.

scActionType

OID: 1.3.6.1.4.1.5951.4.1.1.55.2.1.1.5 The type of action that Citrix ADC takes when initiating on-hold.

scAlternateContentServiceName

OID: 1.3.6.1.4.1.5951.4.1.1.55.2.1.1.6 The alternate service name for the content.

scRuleName

OID: 1.3.6.1.4.1.5951.4.1.1.55.2.1.1.7 The rule that the Citrix ADC matches with the incoming request.

scAlternateContentPath

OID: 1.3.6.1.4.1.5951.4.1.1.55.2.1.1.8 The alternate path for the content.

sslCertKeyTable

OID: 1.3.6.1.4.1.5951.4.1.1.56.1 The ssl certificate key pair configuration information This is indexed on the sslCertKeyName.

sslCertKeyName

OID: 1.3.6.1.4.1.5951.4.1.1.56.1.1.1 The certificate key pair Name.

sslCertPath

OID: 1.3.6.1.4.1.5951.4.1.1.56.1.1.2 The certificate path.

sslKeyPath

OID: 1.3.6.1.4.1.5951.4.1.1.56.1.1.3 The private key path.

sslInputFormat

OID: 1.3.6.1.4.1.5951.4.1.1.56.1.1.4 The input format of the certificate key pair.

sslDaysToExpire

OID: 1.3.6.1.4.1.5951.4.1.1.56.1.1.5 Number of days remaining for the certificate to expire.

sslCrlTable

OID: 1.3.6.1.4.1.5951.4.1.1.56.2 The ssl CRL configuration information This is indexed on the sslCrlName .

sslCrlName

OID: 1.3.6.1.4.1.5951.4.1.1.56.2.1.1 The name of CRL.

sslCrlPath

OID: 1.3.6.1.4.1.5951.4.1.1.56.2.1.2 The CRL path.

sslCrlInputFormat

OID: 1.3.6.1.4.1.5951.4.1.1.56.2.1.3 The input format of CRL.

sslCrlValidity

OID: 1.3.6.1.4.1.5951.4.1.1.56.2.1.4 The validity state of CRL.

sslCipherGroupTable

OID: 1.3.6.1.4.1.5951.4.1.1.56.3 The Cipher group configuration information This is indexed on the sslCipherGroupName and sslCipherName](#sslCipherName)](#)](#)](#) .

sslCipherGroupName

OID: 1.3.6.1.4.1.5951.4.1.1.56.3.1.1 The Cipher group name.

sslCipherName

OID: 1.3.6.1.4.1.5951.4.1.1.56.3.1.2 The Cipher name.

sslCipherDesc

OID: 1.3.6.1.4.1.5951.4.1.1.56.3.1.3 The Cipher description.

dosPolicyTable

OID: 1.3.6.1.4.1.5951.4.1.1.57.1 The dos policy configuration table This is indexed on the dosPolicyName .

dosPolicyName

OID: 1.3.6.1.4.1.5951.4.1.1.57.1.1.1 Name of the policy

thresholdValue

OID: 1.3.6.1.4.1.5951.4.1.1.57.1.1.2 Threshold surge count to detect an attack, for this DosPolicy

dosPolicyStatistics

OID: 1.3.6.1.4.1.5951.4.1.1.57.2 This provides information about DOS Policy related statistics in the Netscaler product.

dosTotConditionTriggered

OID: 1.3.6.1.4.1.5951.4.1.1.57.2.1 Number of times the Citrix ADC triggered the DOS JavaScript due to a condition match.

dosTotValidCookies

OID: 1.3.6.1.4.1.5951.4.1.1.57.2.2 Number of clients from whom the Citrix ADC received a valid DOS cookie.

dosTotDosPriorityClients

OID: 1.3.6.1.4.1.5951.4.1.1.57.2.3 Number of valid clients that were given DOS priority.

dosAvgValidClients

OID: 1.3.6.1.4.1.5951.4.1.1.57.2.4 Average number of DOS clients that returned a valid DOS cookie.

dosAvgDospriClients

OID: 1.3.6.1.4.1.5951.4.1.1.57.2.5 Average number of clients that were given DOS priority.

nsExpressionTable

OID: 1.3.6.1.4.1.5951.4.1.1.58 Expression related configuration This is indexed on the expressionName.

expressionName

OID: 1.3.6.1.4.1.5951.4.1.1.58.1.1 Name of the expression.

expressionTotalHits

OID: 1.3.6.1.4.1.5951.4.1.1.58.1.2 Total number of hits to this expression.

pqPolicyConfigTable

OID: 1.3.6.1.4.1.5951.4.1.1.59.1 The priority queuing policy configuration table This is indexed on the pqName.

pqName

OID: 1.3.6.1.4.1.5951.4.1.1.59.1.1.1 The name of the PQ policy bound to Load Balancing vserver.

pqRuleName

OID: 1.3.6.1.4.1.5951.4.1.1.59.1.1.2 The Rule Name configuration for PQ policy.

pqQdepthThreshold

OID: 1.3.6.1.4.1.5951.4.1.1.59.1.1.3 The vip threshold value for qdepth in PQ policy.

pqPolQdepthThreshold

OID: 1.3.6.1.4.1.5951.4.1.1.59.1.1.4 The policy threshold value for qdepth in PQ policy.

pqPriority

OID: 1.3.6.1.4.1.5951.4.1.1.59.1.1.5 The priority of this PQ policy.

pqPolicyWeight

OID: 1.3.6.1.4.1.5951.4.1.1.59.1.1.6 The weight of this PQ policy.

pqPolicyStatistics

OID: 1.3.6.1.4.1.5951.4.1.1.59.2 This provides information about Priority Queuing Policy related statistics in the Netscaler product.

pqTotalPolicyMatches

OID: 1.3.6.1.4.1.5951.4.1.1.59.2.1 Number of times the Citrix ADC matched an incoming request using any priority queuing policy.

pqTotalThresholdFailed

OID: 1.3.6.1.4.1.5951.4.1.1.59.2.2 Number of times the Citrix ADC failed to match an incoming request to any of priority queing policy.

pqPriority1Requests

OID: 1.3.6.1.4.1.5951.4.1.1.59.2.3 Number of priority 1 requests that the Citrix ADC received.

pqPriority2Requests

OID: 1.3.6.1.4.1.5951.4.1.1.59.2.4 Number of priority 2 requests that the Citrix ADC received.

pqPriority3Requests

OID: 1.3.6.1.4.1.5951.4.1.1.59.2.5 Number of priority 3 requests that the Citrix ADC received.

crPolicyMapConfigTable

OID: 1.3.6.1.4.1.5951.4.1.1.60.1 The CR map configuration information This is indexed on the crMapName .

crMapName

OID: 1.3.6.1.4.1.5951.4.1.1.60.1.1.1 The name of the map policy.

crMapSrcName

OID: 1.3.6.1.4.1.5951.4.1.1.60.1.1.2 The name of the source domain hosted by the map.

crMapDstName

OID: 1.3.6.1.4.1.5951.4.1.1.60.1.1.3 The name of the destination domain hosted by the map.

crMapSrcUrl

OID: 1.3.6.1.4.1.5951.4.1.1.60.1.1.4 The Url to be modified under the given source domain.

crMapDstUrl

OID: 1.3.6.1.4.1.5951.4.1.1.60.1.1.5 The Url after mapping.

crMapFullName

OID: 1.3.6.1.4.1.5951.4.1.1.60.1.1.6 Full name of the Map policy.

monitorCount

OID: 1.3.6.1.4.1.5951.4.1.1.61 Number of monitors defined on this Citrix ADC.

monitorBindCount

OID: 1.3.6.1.4.1.5951.4.1.1.62 Number of monitor bindings defined on this Citrix ADC.

appFirewallStatistics

OID: 1.3.6.1.4.1.5951.4.1.1.64.1 This provides Application Firewall statistics in the Netscaler product.

appFirewallRequests

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.1 HTTP/HTTPS requests sent to your protected web servers via the Application Firewall.

appFirewallResponses

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.2 HTTP/HTTPS responses sent by your protected web servers via the Application Firewall.

appFirewallAborts

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.3 Incomplete HTTP/HTTPS requests aborted by the client before the Application Firewall could finish processing them.

appFirewallRedirects

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.4

HTTP/HTTPS

OID:requests

appFirewallViolStartURL

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.5 Number of Start URL security check violations seen by the Application Firewall.

appFirewallViolDenyURL

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.6 Number of Deny URL security check violations seen by the Application Firewall.

appFirewallViolBufferOverflow

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.7 Number of Buffer Overflow security check violations seen by the Application Firewall.

appFirewallViolCookie

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.8 Number of Cookie Consistency security check violations seen by the Application Firewall.

appFirewallViolXSS

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.9 Number of HTML Cross-Site Scripting security check violations seen by the Application Firewall.

appFirewallViolSQL

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.10 Number of HTML SQL Injection security check violations seen by the Application Firewall.

appFirewallViolFieldformat

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.11 Number of Field Format security check violations seen by the Application Firewall.

appFirewallViolFieldConsistency

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.12 Number of Field Consistency security check violations seen by the Application Firewall.

appFirewallViolCreditCard

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.13 Number of Credit Card security check violations seen by the Application Firewall.

appFirewallViolSafeObject

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.14 Number of Safe Object security check violations seen by the Application Firewall.

appFirewallTotalViol

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.15 Total number of security check violations seen by the Application Firewall.

appFirewallViolWellformednessViolations

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.16 Number of XML Format security check violations seen by the Application Firewall.

appFirewallViolXdosViolations

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.17 Number of XML Denial-of-Service security check violations seen by the Application Firewall.

appFirewallViolMsgValViolations

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.18 Number of XML Message Validation security check violations seen by the Application Firewall.

appFirewallViolWSIViolations

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.19 Number of Web Services Interoperability (WS-I) security check violations seen by the Application Firewall.

appFirewallViolXmlSqlViolations

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.20 Number of XML SQL Injection security check violations seen by the Application Firewall.

appFirewallViolXmlXssViolations

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.21 Number of XML Cross-Site Scripting (XSS) security check violations seen by the Application Firewall.

appFirewallViolXmlAttachmentViolations

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.22 Number of XML Attachment security check violations seen by the Application Firewall.

appFirewallViolCSRFtag

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.23 Number of Cross Site Request Forgery form tag security check violations seen by the Application Firewall.

appFirewallViolRefererHeader

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.24 Number of Referer Header security check violations seen by the Application Firewall.

appFirewallViolXmlSoapFaultViolations

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.25 Number of requests returning soap:fault from the backend server

appFirewallRet4xx

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.26 Number of requests returning HTTP 4xx from the backend server

appFirewallRet5xx

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.27 Number of requests returning HTTP 5xx from the backend server

appFirewallReqBytes

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.28 Number of bytes transfered for requests

appFirewallResBytes

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.29 Number of bytes transfered for responses

appFirewallLongAvgRespTime

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.30 Average backend response time in milliseconds since reboot

appFirewallShortAvgRespTime

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.31 Average backend response time in milliseconds over the last 7 seconds

appFirewallViolXmlGenViolations

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.32 Number of requests returning XML generic error from the backend server

appFirewallViolSignature

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.33 Number of Signature violations seen by the Application Firewall.

appFirewallTrapsDropped

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.34 AppFirewall SNMP traps dropped due to time limit.

appFirewallViolJsonDos

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.35 Number of JSON Denial-of-Service security check violations seen by the Application Firewall.

appFirewallViolJsonSql

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.36 Number of JSON SQL Injection security check violations seen by the Application Firewall.

appFirewallViolJsonXss

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.37 Number of JSON Cross-Site Scripting (XSS) security check violations seen by the Application Firewall.

appFirewallViolFileUploadTypes

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.38 Number of Field Upload Types security check violations seen by the Application Firewall.

appFirewallViolXMLPayloadContentTypeMismatch

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.39 Number of Mismatched Content-Type in request with XML Payload security check violations seen by the Application Firewall.

appFirewallViolCookieHijack

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.40 Number of Cookie Hijacking security violations seen by the Application Firewall.

appFirewallViolCMD

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.41 Number of HTML CMD Injection security check violations seen by the Application Firewall.

appFirewallPostBodyLimitViolations

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.42 Number of Post Body Limit security check violations seen by the Application Firewall.

appFirewallViolJsonCmd

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.43 Number of JSON Command Injection security check violations seen by the Application Firewall.

appFirewallViolJsonSqlGram

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.44 Number of JSON SQL Injection security check violations (reported using SQL grammar) seen by the Application Firewall.

appFirewallViolSQLGram

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.45 Number of HTML SQL Injection security check violations (using SQL grammar) seen by the Application Firewall.

appFirewallViolGRPC

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.46 Number of gRPC security check violations seen by the Application Firewall.

appFirewallViolCMDGram

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.47 Number of HTML CMD Injection security check violations (using SQL grammar) seen by the Application Firewall.

appFirewallViolJsonCmdGram

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.48 Number of JSON CMD Injection security check violations (reported using CMD grammar) seen by the Application Firewall.

appFirewallViolBlockKeyword

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.49 Number of Block Keyword security check violations seen by the Application Firewall.

appFirewallViolJSONBlockKeyword

OID: 1.3.6.1.4.1.5951.4.1.1.64.1.50 Number of JSON Block Keyword security check violations seen by the Application Firewall.

appfwProfileTable

OID: 1.3.6.1.4.1.5951.4.1.1.64.2

This is indexed on the appfwprofileName.

appfwprofileName

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.1 The name of the Application Firewall profile

appfwappFirewallRequestsPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.2 HTTP/HTTPS requests sent to your protected web servers via the Application Firewall.

appfwappFirewallResponsesPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.3 HTTP/HTTPS responses sent by your protected web servers via the Application Firewall.

appfwappFirewallAbortsPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.4 Incomplete HTTP/HTTPS requests aborted by the client before the Application Firewall could finish processing them.

appfwappFirewallRedirectsPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.5

HTTP/HTTPS

OID:requests

appfwappFirewallViolStartURLPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.6 Number of Start URL security check violations seen by the Application Firewall.

appfwappFirewallViolDenyURLPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.7 Number of Deny URL security check violations seen by the Application Firewall.

appfwappFirewallViolRefererHeaderPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.8 Number of Referer Header security check violations seen by the Application Firewall.

appfwappFirewallViolBufferOverflowPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.9 Number of Buffer Overflow security check violations seen by the Application Firewall.

appfwappFirewallViolCSRFtagPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.10 Number of Cross Site Request Forgery form tag security check violations seen by the Application Firewall.

appfwappFirewallViolCookiePerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.11 Number of Cookie Consistency security check violations seen by the Application Firewall.

appfwappFirewallViolXSSPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.12 Number of HTML Cross-Site Scripting security check violations seen by the Application Firewall.

appfwappFirewallViolSQLPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.13 Number of HTML SQL Injection security check violations seen by the Application Firewall.

appfwappFirewallViolFieldformatPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.14 Number of Field Format security check violations seen by the Application Firewall.

appfwappFirewallViolFieldConsistencyPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.15 Number of Field Consistency security check violations seen by the Application Firewall.

appfwappFirewallViolCreditCardPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.16 Number of Credit Card security check violations seen by the Application Firewall.

appfwappFirewallViolSafeObjectPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.17 Number of Safe Object security check violations seen by the Application Firewall.

appfwappFirewallViolWellformednessViolationsPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.18 Number of XML Format security check violations seen by the Application Firewall.

appfwappFirewallViolXdosViolationsPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.19 Number of XML Denial-of-Service security check violations seen by the Application Firewall.

appfwappFirewallViolMsgValViolationsPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.20 Number of XML Message Validation security check violations seen by the Application Firewall.

appfwappFirewallViolWSIViolationsPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.21 Number of Web Services Interoperability (WS-I) security check violations seen by the Application Firewall.

appfwappFirewallViolXmlSqlViolationsPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.22 Number of XML SQL Injection security check violations seen by the Application Firewall.

appfwappFirewallViolXmlXssViolationsPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.23 Number of XML Cross-Site Scripting (XSS) security check violations seen by the Application Firewall.

appfwappFirewallViolXmlAttachmentViolationsPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.24 Number of XML Attachment security check violations seen by the Application Firewall.

appfwappFirewallTotalViolPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.25 Number of violations seen by the application firewall on per profile basis

appfwappFirewallRet4xxPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.26 Number of requests returning HTTP 4xx from the backend server

appfwappFirewallRet5xxPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.27 Number of requests returning HTTP 5xx from the backend server

appfwappFirewallViolXmlSoapFaultViolationsPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.28 Number of requests returning soap:fault from the backend server

appfwappFirewallReqBytesPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.29 Number of bytes transfered for requests

appfwappFirewallResBytesPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.30 Number of bytes transfered for responses

appfwappFirewallLongAvgRespTimePerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.31 Average backend response time in milliseconds since reboot

appfwappFirewallShortAvgRespTimePerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.32 Average backend response time in milliseconds over the last 7 seconds

appfwappFirewallViolXmlGenericViolationsPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.33 Number of requests returning XML generic violation from the backend server

appfwappFirewallViolSignaturePerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.34 Number of Signature violations seen by the Application Firewall.

appfwappFirewallViolJsonDosPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.35 Number of JSON Denial-of-Service security check violations seen by the Application Firewall.

appfwappFirewallViolJsonSqlPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.36 Number of JSON SQL Injection security check violations seen by the Application Firewall.

appfwappFirewallViolJsonXssPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.37 Number of JSON Cross-Site Scripting (XSS) security check violations seen by the Application Firewall.

appfwappFirewallViolFileUploadTypesPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.38 Number of Field Upload Types security check violations seen by the Application Firewall.

appfwappFirewallXMLPayloadContentTypeMismatchPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.39 Number of Mismatched Content-Type in request with XML Payload security check violations seen by the Application Firewall.

appfwappFirewallViolCookieHijackPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.40 Number of Cookie Hijacking security violations seen by the Application Firewall.

appfwappFirewallViolCMDPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.41 Number of HTML Command Injection security check violations seen by the Application Firewall.

appfwappFirewallPostBodyLimitViolationsPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.42 Number of Post Body Limit security check violations seen by the Application Firewall.

appfwappFirewallViolJsonCmdPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.43 Number of JSON Command Injection security check violations seen by the Application Firewall.

appfwappFirewallViolJsonSqlGramPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.44 Number of JSON SQL Injection security check violations (reported by SQL grammar) seen by the Application Firewall.

appfwappFirewallViolSQLGramPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.45 Number of HTML SQL Injection security check violations (reported by SQL grammar) seen by the Application Firewall.

appfwProfileFullName

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.46 The full name of the Application Firewall profile

appfwappFirewallViolJsonCmdGramPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.47 Number of JSON CMD Injection security check violations (reported by CMD grammar) seen by the Application Firewall.

appfwappFirewallViolCMDGramPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.48 Number of HTML CMD Injection security check violations (reported by CMD grammar) seen by the Application Firewall.

appfwappFirewallViolBlockKeywordPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.49 Number of HTML Block Keyword security check violations seen by the Application Firewall.

appfwappFirewallViolJSONBlockKeywordPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.64.2.1.50 Number of JSON Block Keyword security check violations seen by the Application Firewall.

nsRnatGlobalStats

OID: 1.3.6.1.4.1.5951.4.1.1.65.1 This provides statistics related to all RNAT sessions.

rnatTotRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.65.1.1 Bytes received during RNAT sessions.

rnatTotTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.65.1.2 Bytes sent during RNAT sessions.

rnatTotRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.65.1.3 Packets received during RNAT sessions.

rnatTotTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.65.1.4 Packets sent during RNAT sessions.

rnatTotTxSyn

OID: 1.3.6.1.4.1.5951.4.1.1.65.1.5 Requests for connections sent during RNAT sessions.

rnatCurSessions

OID: 1.3.6.1.4.1.5951.4.1.1.65.1.6 Currently active RNAT sessions.

nsRnatPerIPStatsTable

OID: 1.3.6.1.4.1.5951.4.1.1.65.2 This table contains statistics related to rnat for the natip This is indexed on the ipAddr.

ipRnatTotRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.65.2.1.1 Bytes received on this IP address during RNAT sessions.

ipRnatTotTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.65.2.1.2 Bytes sent from this IP address during RNAT sessions.

ipRnatTotRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.65.2.1.3 Packets received on this IP address during RNAT sessions.

ipRnatTotTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.65.2.1.4 Packets sent from this IP address during RNAT sessions.

ipRnatTotTxSyn

OID: 1.3.6.1.4.1.5951.4.1.1.65.2.1.5 Requests for connections sent from this IP address during RNAT sessions.

ipRnatCurSessions

OID: 1.3.6.1.4.1.5951.4.1.1.65.2.1.6 Currently active RNAT sessions started from this IP address.

nsSslVpnStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.66 This provides information about SSL-VPN related statistics

indexHtmlHit

OID: 1.3.6.1.4.1.5951.4.1.1.66.1 Number of requests for VPN login page.

indexHtmlNoServed

OID: 1.3.6.1.4.1.5951.4.1.1.66.2 Number of failures to display VPN login page.

cfgHtmlServed

OID: 1.3.6.1.4.1.5951.4.1.1.66.3 Number of client configuration requests received by VPN server.

dnsReqHit

OID: 1.3.6.1.4.1.5951.4.1.1.66.4 Number of DNS queries resolved by VPN server.

winsRequestHit

OID: 1.3.6.1.4.1.5951.4.1.1.66.5 Number of WINS queries resolved by VPN server.

csRequestHit

OID: 1.3.6.1.4.1.5951.4.1.1.66.6 Number of SSL VPN tunnels formed between VPN server and client.

csNonHttpProbeHit

OID: 1.3.6.1.4.1.5951.4.1.1.66.7 Number of probes from VPN to back-end non-HTTP servers that have been accessed by the VPN client.

csHttpProbeHit

OID: 1.3.6.1.4.1.5951.4.1.1.66.8 Number of probes from VPN to back-end HTTP servers that have been accessed by the VPN client.

totalCsConnSucc

OID: 1.3.6.1.4.1.5951.4.1.1.66.9 Number of successful probes to all back-end servers.

totalFsRequest

OID: 1.3.6.1.4.1.5951.4.1.1.66.10 Number of file system requests received by VPN server.

iipDisabledMIPdisabled

OID: 1.3.6.1.4.1.5951.4.1.1.66.11 Both IIP and SNIP is disabled.

iipFailedMIPdisabled

OID: 1.3.6.1.4.1.5951.4.1.1.66.12 Number of times IIP assignment failed and SNIP is disabled.

iipDisabledMIPused

OID: 1.3.6.1.4.1.5951.4.1.1.66.13 Number of times SNIP is used as IIP is disabled.

iipFailedMIPused

OID: 1.3.6.1.4.1.5951.4.1.1.66.14 Number of times SNIP is used as IIP assignment failed.

socksMethReqRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.66.15 Number of received SOCKS method request.

socksMethReqSent

OID: 1.3.6.1.4.1.5951.4.1.1.66.16 Number of sent SOCKS method request.

socksMethRespRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.66.17 Number of received SOCKS method response.

socksMethRespSent

OID: 1.3.6.1.4.1.5951.4.1.1.66.18 Number of sent SOCKS method response.

socksConnReqRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.66.19 Number of received SOCKS connect request.

socksConnReqSent

OID: 1.3.6.1.4.1.5951.4.1.1.66.20 Number of sent SOCKS connect request.

socksConnRespRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.66.21 Number of received SOCKS connect response.

socksConnRespSent

OID: 1.3.6.1.4.1.5951.4.1.1.66.22 Number of sent SOCKS connect response.

socksServerError

OID: 1.3.6.1.4.1.5951.4.1.1.66.23 Number of SOCKS server error.

socksClientError

OID: 1.3.6.1.4.1.5951.4.1.1.66.24 Number of SOCKS client error.

staConnSuccess

OID: 1.3.6.1.4.1.5951.4.1.1.66.25 Number of STA connection success.

staConnFailure

OID: 1.3.6.1.4.1.5951.4.1.1.66.26 Number of STA connection failure.

cpsConnSuccess

OID: 1.3.6.1.4.1.5951.4.1.1.66.27 Number of CPS connection success.

cpsConnFailure

OID: 1.3.6.1.4.1.5951.4.1.1.66.28 Number of CPS connection failure.

staRequestSent

OID: 1.3.6.1.4.1.5951.4.1.1.66.29 Number of STA request sent.

staResponseRecvd

OID: 1.3.6.1.4.1.5951.4.1.1.66.30 Number of STA response received.

icaLicenseFailure

OID: 1.3.6.1.4.1.5951.4.1.1.66.31 Number of ICA license failure.

staRenewSent

OID: 1.3.6.1.4.1.5951.4.1.1.66.32 Number of STA renew requests sent.

staRenewRecvd

OID: 1.3.6.1.4.1.5951.4.1.1.66.33 Number of STA renew response received.

staReassErr

OID: 1.3.6.1.4.1.5951.4.1.1.66.34 Number of STA response reassembly errors.

staRnewNoClnt

OID: 1.3.6.1.4.1.5951.4.1.1.66.35 Number of STA renew repsonse for missing clients.

staRenewNoRfsh

OID: 1.3.6.1.4.1.5951.4.1.1.66.36 Number of STA renew response missing refesh values.

staValidNoClnt

OID: 1.3.6.1.4.1.5951.4.1.1.66.37 Number of STA validate response for clients that have already closed.

staValidNoEst

OID: 1.3.6.1.4.1.5951.4.1.1.66.38 Number of STA validate responses for clients not in TCP ESTABLISHED state.

staMonSent

OID: 1.3.6.1.4.1.5951.4.1.1.66.39 Number of STA monitor requests sent.

staMonRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.66.40 Number of STA monitor responses recieved.

staMonSucc

OID: 1.3.6.1.4.1.5951.4.1.1.66.41 Number of STA monitor successful responses.

staMonFail

OID: 1.3.6.1.4.1.5951.4.1.1.66.42 Number of STA monitor failed responses.

iipSpilloverMIPused

OID: 1.3.6.1.4.1.5951.4.1.1.66.43 Number of times SNIP is used on IIP Spillover.

iPv6tov4FindIPv6MapErr

OID: 1.3.6.1.4.1.5951.4.1.1.66.44 Number of IPv6toIPv4 find IPv6 mapping errors.

iPv6toV4MapInsertErr

OID: 1.3.6.1.4.1.5951.4.1.1.66.45 Number of Ipv6 to Ipv4 mapping Insert Errors.

parseIPv6AddressErr

OID: 1.3.6.1.4.1.5951.4.1.1.66.46 Errors in parsing for Ipv6 address from address string.

dtlsStaValidation

OID: 1.3.6.1.4.1.5951.4.1.1.66.47 Number of STA validation requests on DTLS

dtlsStaValidationError

OID: 1.3.6.1.4.1.5951.4.1.1.66.48 Number of STA validation request errors on DTLS

dtlsStaReconnectTktReq

OID: 1.3.6.1.4.1.5951.4.1.1.66.49 Number of STA Reconnet ticket requests on DTLS

dtlsStaPostResponseSuccess

OID: 1.3.6.1.4.1.5951.4.1.1.66.50 Number of Successfull STA Validations done on DTLS

dtlsStaPostResponseError

OID: 1.3.6.1.4.1.5951.4.1.1.66.51 Number of errors during STA Validations on DTLS

vpnLicenseFail

OID: 1.3.6.1.4.1.5951.4.1.1.66.52 Number of users not able to login because of license unavailability.

svpnhttpdTotalRequests

OID: 1.3.6.1.4.1.5951.4.1.1.66.53 Total number of requests from VPN to Apache

svpnhttpdTotalResponses

OID: 1.3.6.1.4.1.5951.4.1.1.66.54 Total number of responses from Apache for VPN

svpnhttpdTotalRequestsCacheHits

OID: 1.3.6.1.4.1.5951.4.1.1.66.55 Total number of vpn requests to Apache hitting cache

svpnhttpdCurServerConnectionsOpen

OID: 1.3.6.1.4.1.5951.4.1.1.66.56 Number of current VPN to Apache open server connections

nsAaaStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.67 This provides information about AAA related statistics

aaaAuthFail

OID: 1.3.6.1.4.1.5951.4.1.1.67.1 Count of authentication failures.

aaaAuthSuccess

OID: 1.3.6.1.4.1.5951.4.1.1.67.2 Count of authentication successes.

aaaAuthNonHttpFail

OID: 1.3.6.1.4.1.5951.4.1.1.67.3 Count of non HTTP connections that failed authorization.

aaaAuthOnlyHttpFail

OID: 1.3.6.1.4.1.5951.4.1.1.67.4 Count of HTTP connections that failed authorization.

aaaAuthNonHttpSuccess

OID: 1.3.6.1.4.1.5951.4.1.1.67.5 Count of non HTTP connections that succeeded authorization.

aaaAuthOnlyHttpSuccess

OID: 1.3.6.1.4.1.5951.4.1.1.67.6 Count of HTTP connections that succeeded authorization.

aaaTotSessions

OID: 1.3.6.1.4.1.5951.4.1.1.67.7 Count of all SmartAccess AAA sessions.

aaaTotSessionTimeout

OID: 1.3.6.1.4.1.5951.4.1.1.67.8 Count of AAA sessions that have timed out.

aaaCurSessions

OID: 1.3.6.1.4.1.5951.4.1.1.67.9 Count of current SmartAccess AAA sessions.

aaaCurICASessions

OID: 1.3.6.1.4.1.5951.4.1.1.67.10 Count of current Basic ICA only sessions.

aaaCurTMSessions

OID: 1.3.6.1.4.1.5951.4.1.1.67.11 Count of current AAATM sessions.

aaaTotTMSessions

OID: 1.3.6.1.4.1.5951.4.1.1.67.12 Count of all AAATM sessions.

aaaCurICAOnlyConn

OID: 1.3.6.1.4.1.5951.4.1.1.67.13 Count of current Basic ICA only connections.

aaaCurICAConn

OID: 1.3.6.1.4.1.5951.4.1.1.67.14 Count of current SmartAccess ICA connections.

aaaTotWafBlock

OID: 1.3.6.1.4.1.5951.4.1.1.67.15 Total Number of Requests that are blocked as part of Appfw Validation for AAA

aaatmTotWafBlock

OID: 1.3.6.1.4.1.5951.4.1.1.67.16 Total Number of Requests that are blocked as part of Appfw Validation for AAATM

nsGlobalConfigSettings

OID: 1.3.6.1.4.1.5951.4.1.1.68 This provides information about global configurations of Netscaler.

webServerHttpPorts

OID: 1.3.6.1.4.1.5951.4.1.1.68.1 The HTTP ports on the Web server. System performs connection off-load for any client request that has a destination port matching one of these configured ports.

maxTcpConnections

OID: 1.3.6.1.4.1.5951.4.1.1.68.2 The maximum number of connections that will be made from the system to the web server(s) attached to it. This value is applied globally to all attached servers.

maxReqPerConnection

OID: 1.3.6.1.4.1.5951.4.1.1.68.3 The maximum number of requests that the system can pass on a particular connection between the system and a server attached to it. If the Value is zero, then it allows an unlimited number of requests to be passed.

cipInsertionStatus

OID: 1.3.6.1.4.1.5951.4.1.1.68.4 This represents the option to control (enable or disable) the insertion of the actual client IP address into the HTTP header request passed from the client to any of the servers attached to the system. The passed address can then be accessed through a minor modification to the server. If cipHeader is specified, it will be used as the client IP header. If it is not specified, then the value that has been set by the set ns config CLI command will be used as the client IP header.

cipInsertionHeader

OID: 1.3.6.1.4.1.5951.4.1.1.68.5 This represents the text that will be used as the client IP header.

cookieVersionInserted

OID: 1.3.6.1.4.1.5951.4.1.1.68.6 The version of the cookie inserted by the system.

minPathMTU

OID: 1.3.6.1.4.1.5951.4.1.1.68.7 The minimum Path MTU of the system.

mtuEntryTimeoutValue

OID: 1.3.6.1.4.1.5951.4.1.1.68.8 The timeout value of MTU entries.

ftpPortRange

OID: 1.3.6.1.4.1.5951.4.1.1.68.9 The Port range configured for FTP services.

piPolicyTable

OID: 1.3.6.1.4.1.5951.4.1.1.69.1 The policy relationship table This is indexed on the piPolName .

piPolName

OID: 1.3.6.1.4.1.5951.4.1.1.69.1.1.1 Encoded name of the PI policy

piPolicyHits

OID: 1.3.6.1.4.1.5951.4.1.1.69.1.1.2 Number of hits on the policy

piPolicyUndefHits

OID: 1.3.6.1.4.1.5951.4.1.1.69.1.1.3 Number of undef hits on the policy

piPolFullName

OID: 1.3.6.1.4.1.5951.4.1.1.69.1.1.4 Full name of the PI policy

nsInetAddressTable

OID: 1.3.6.1.4.1.5951.4.1.1.70 This table contains information about the IPv6 addresses configured on the Citrix ADC. This is indexed on the nsInetAddressType and nsInetAddress](#nsInetAddress)](#)](#)](#) .

nsInetAddressType

OID: 1.3.6.1.4.1.5951.4.1.1.70.1.1 The address type of nsInetAddress

nsInetAddress

OID: 1.3.6.1.4.1.5951.4.1.1.70.1.2 This represents an IPv4/v6 address configured on the Citrix ADC

nsInetMaskLenth

OID: 1.3.6.1.4.1.5951.4.1.1.70.1.3 This represents netmask length.

nsInetType

OID: 1.3.6.1.4.1.5951.4.1.1.70.1.4 This represents the IP address type

nsInetMode

OID: 1.3.6.1.4.1.5951.4.1.1.70.1.5 This represents the IP address mode

nsInetFreePorts

OID: 1.3.6.1.4.1.5951.4.1.1.70.1.6 This represents the number of unused ports free on this IP

nsInetVlan

OID: 1.3.6.1.4.1.5951.4.1.1.70.1.7 The vlan to which this ip address is bound.

nsInetBridgeGroup

OID: 1.3.6.1.4.1.5951.4.1.1.70.1.8 The bridge group to which this ip address is bound.

nsInetVxlan

OID: 1.3.6.1.4.1.5951.4.1.1.70.1.9 The vxlan to which this ip address is bound.

nsNicStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.71 This provides statistical information about the total number of megabits received/transmitted on the Network Interfaces configured in the Netscaler product.

allNicTotRxMbits

OID: 1.3.6.1.4.1.5951.4.1.1.71.1 Number of megabits received by the Citrix ADC.

allNicTotTxMbits

OID: 1.3.6.1.4.1.5951.4.1.1.71.2 Number of megabits transmitted by the Citrix ADC.

allNicTotRxRate

OID: 1.3.6.1.4.1.5951.4.1.1.71.3 Number of bits received per sec by the Citrix ADC.

allNicTotRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.71.4 Number of packets received by the Citrix ADC.

allNicTotRxPktRate

OID: 1.3.6.1.4.1.5951.4.1.1.71.5 Number of packets received per sec by the Citrix ADC.

clusterTable

OID: 1.3.6.1.4.1.5951.4.1.1.72 The cluster table. This is indexed on the clnodeID.

clnodeID

OID: 1.3.6.1.4.1.5951.4.1.1.72.1.1 This represents the unique id of the cluster node

clPeerIP

OID: 1.3.6.1.4.1.5951.4.1.1.72.1.2 This represents the IP address of the cluster node

clNodeIP

OID: 1.3.6.1.4.1.5951.4.1.1.72.1.3 This represents the ip of the cluster node for which notification is being sent

clAdminState

OID: 1.3.6.1.4.1.5951.4.1.1.72.1.4 Admin State of the node in the cluster.

clMasterState

OID: 1.3.6.1.4.1.5951.4.1.1.72.1.5 Operational state of the cluster node.

clNodeHealth

OID: 1.3.6.1.4.1.5951.4.1.1.72.1.6 Health of the node in the cluster.

clNodeEffectiveHealth

OID: 1.3.6.1.4.1.5951.4.1.1.72.1.7 Health of the cluster node.

clSyncState

OID: 1.3.6.1.4.1.5951.4.1.1.72.1.8 Sync state of the cluster node.

clNodeViewQuorum

OID: 1.3.6.1.4.1.5951.4.1.1.72.1.9 This represents whether the node view of cluster has quorum or not

clNodeHealthReason

OID: 1.3.6.1.4.1.5951.4.1.1.72.1.10 This represents the reason for bad health of the cluster node

nsClusterStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.73 This provides information about the Cluster feature in the Netscaler product.

clViewLeader

OID: 1.3.6.1.4.1.5951.4.1.1.73.1 NSIP address of the Configuration Coordinator of the cluster.

nsInatGlobalStats

OID: 1.3.6.1.4.1.5951.4.1.1.74.1 This provides statistics related to all INAT sessions.

nat46TotTcp46

OID: 1.3.6.1.4.1.5951.4.1.1.74.1.1 Total TCP packets translated (V4->v6).

nat46TotUdp46

OID: 1.3.6.1.4.1.5951.4.1.1.74.1.2 Total UDP packets translated (V4->v6).

nat46TotIcmp46

OID: 1.3.6.1.4.1.5951.4.1.1.74.1.3 Total ICMP packets translated (V4->v6).

nat46TotDrop46

OID: 1.3.6.1.4.1.5951.4.1.1.74.1.4 Total IPV4 packets dropped.

nat46TotTcp64

OID: 1.3.6.1.4.1.5951.4.1.1.74.1.5 Total TCP packets translated (V6->v4).

nat46TotUdp64

OID: 1.3.6.1.4.1.5951.4.1.1.74.1.6 Total UDP packets translated (V6->v4).

nat46TotIcmp64

OID: 1.3.6.1.4.1.5951.4.1.1.74.1.7 Total ICMP packets translated (V6->v4).

nat46TotDrop64

OID: 1.3.6.1.4.1.5951.4.1.1.74.1.8 Total IPV6 packets dropped.

nsInatPerNat46StatsTable

OID: 1.3.6.1.4.1.5951.4.1.1.74.2 This provides statistics related to per nat46 rule

This is indexed on the

OID: ``

inatname

OID: 1.3.6.1.4.1.5951.4.1.1.74.2.1.1 The name of the INAT

inatNat46Tcp46

OID: 1.3.6.1.4.1.5951.4.1.1.74.2.1.2 TCP packets translated (V4->v6).

inatNat46Udp46

OID: 1.3.6.1.4.1.5951.4.1.1.74.2.1.3 UDP packets translated (V4->v6).

inatNat46Icmp46

OID: 1.3.6.1.4.1.5951.4.1.1.74.2.1.4 ICMP packets translated (V4->v6).

inatNat46Drop46

OID: 1.3.6.1.4.1.5951.4.1.1.74.2.1.5 IPV4 packets dropped.

inatNat46Tcp64

OID: 1.3.6.1.4.1.5951.4.1.1.74.2.1.6 TCP packets translated (V6->v4).

inatNat46Udp64

OID: 1.3.6.1.4.1.5951.4.1.1.74.2.1.7 UDP packets translated (V6->v4).

inatNat46Icmp64

OID: 1.3.6.1.4.1.5951.4.1.1.74.2.1.8 ICMP packets translated (V6->v4).

inatNat46Drop64

OID: 1.3.6.1.4.1.5951.4.1.1.74.2.1.9 IPV6 packets dropped.

nsInatPerNatStatsTable

OID: 1.3.6.1.4.1.5951.4.1.1.74.3 This provides statistics related to per inat session

This is indexed on the

OID:](#)

inat44name

OID: 1.3.6.1.4.1.5951.4.1.1.74.3.1.1 The name of the INAT

inatTotHits

OID: 1.3.6.1.4.1.5951.4.1.1.74.3.1.2 INAT total sessions

inatCurSessions

OID: 1.3.6.1.4.1.5951.4.1.1.74.3.1.3 INAT current sessions

inatTotReceiveBytes

OID: 1.3.6.1.4.1.5951.4.1.1.74.3.1.4 INAT total Received Bytes

inatTotSentBytes

OID: 1.3.6.1.4.1.5951.4.1.1.74.3.1.5 INAT total Sent Bytes

inatTotpktreceived

OID: 1.3.6.1.4.1.5951.4.1.1.74.3.1.6 INAT total Packets Received

inatTotpktsent

OID: 1.3.6.1.4.1.5951.4.1.1.74.3.1.7 INAT total Packets Sent

nsInatSessionGlobalStats

OID: 1.3.6.1.4.1.5951.4.1.1.74.4 This provides statistics related to all INATsessions.

globalInatHits

OID: 1.3.6.1.4.1.5951.4.1.1.74.4.1 Total INAT Session hits

globalInatCurSessions

OID: 1.3.6.1.4.1.5951.4.1.1.74.4.2 Total INAT current sessions

globalInatReceiveBytes

OID: 1.3.6.1.4.1.5951.4.1.1.74.4.3 Total INAT Received Bytes

globalInatTotSentBytes

OID: 1.3.6.1.4.1.5951.4.1.1.74.4.4 Total INAT Sent Bytes

globalInatPktReceived

OID: 1.3.6.1.4.1.5951.4.1.1.74.4.5 Total INAT Packets Received

globalInatPktSent

OID: 1.3.6.1.4.1.5951.4.1.1.74.4.6 Total INAT Packets Sent

nsNat64GlobalStats

OID: 1.3.6.1.4.1.5951.4.1.1.75.1 This provides statistics related to all NAT64 sessions.

nat64TotUdpSessions

OID: 1.3.6.1.4.1.5951.4.1.1.75.1.1 Total number of UDP sessions created by NAT64.

nat64TotTcpSessions

OID: 1.3.6.1.4.1.5951.4.1.1.75.1.2 Total number of TCP sessions created by NAT64.

nat64TotSessions

OID: 1.3.6.1.4.1.5951.4.1.1.75.1.3 Total number of sessions created by NAT64.

nat64TotIcmpSessions

OID: 1.3.6.1.4.1.5951.4.1.1.75.1.4 Total number of ICMP sessions created by NAT64.

nsIp6StatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.76 This provides information about IPv6 related statistics in the Netscaler product.

ipv6TotRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.76.1 IPv6 packets received.

ipv6TotTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.76.2 IPv6 packets transmitted

ipv6TotRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.76.3 Bytes of IPv6 data received.

ipv6TotTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.76.4 Bytes of IPv6 data transmitted.

ipv6FragTotRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.76.5 IPv6 fragments received.

ipv6FragTotPktsForward

OID: 1.3.6.1.4.1.5951.4.1.1.76.6 IPv6 fragments forwarded to the client or server without reassembly.

ipv6FragTotPktsProcessNoReass

OID: 1.3.6.1.4.1.5951.4.1.1.76.7 IPv6 fragments processed without reassembly.

ipv6ErrHdr

OID: 1.3.6.1.4.1.5951.4.1.1.76.8 Packets received that contain an error in one or more components of the IPv6 header.

ipv6LandAttack

OID: 1.3.6.1.4.1.5951.4.1.1.76.9 Land-attack packets received. The source and destination addresses are the same. If not dropped, these packets can lock up the appliance.

ipv6FragZeroLenPkt

OID: 1.3.6.1.4.1.5951.4.1.1.76.10 Packets received with a fragment length of 0 bytes.

ipv6TotIcmpFragPkts

OID: 1.3.6.1.4.1.5951.4.1.1.76.11 Number of ICMPV6 fragmented packets.

ipv6TotLookupDone

OID: 1.3.6.1.4.1.5951.4.1.1.76.12 Total number of nd6 lookup done.

ipv6TotLookupFailed

OID: 1.3.6.1.4.1.5951.4.1.1.76.13 Total number of nd6 lookup failed.

ipv6TotStaticRoutes

OID: 1.3.6.1.4.1.5951.4.1.1.76.14 Total number of static ipv6 routes.

ipv6TotDynamicRoutes

OID: 1.3.6.1.4.1.5951.4.1.1.76.15 Total number of dynamic ipv6 routes.

ipv6TotNeigborDiscovered

OID: 1.3.6.1.4.1.5951.4.1.1.76.16 Total number of nd6 entries both dynamic and static.

ipv6TotIpv6To4Conversions

OID: 1.3.6.1.4.1.5951.4.1.1.76.17 Total number of ipv6 to v4 conversion done.

ipv6TotIpv4To6Conversions

OID: 1.3.6.1.4.1.5951.4.1.1.76.18 Total number of ipv4 to v6 conversion done.

ipv6TotTcpConnection

OID: 1.3.6.1.4.1.5951.4.1.1.76.19 TCP connections over IPv6.

ipv6TotNonTcpConnection

OID: 1.3.6.1.4.1.5951.4.1.1.76.20 Non TCP connections over IPv6.

nsTdInetAddressTable

OID: 1.3.6.1.4.1.5951.4.1.1.77 This table contains information about the non-default Td IP Addresses configured on the Citrix ADC. This is indexed on the nsTdInetId and nsTdInetAddressType and nsTdInetAddress](#)](#) .

nsTdInetId

OID: 1.3.6.1.4.1.5951.4.1.1.77.1.1 This represents a traffic domain ID

nsTdInetAddressType

OID: 1.3.6.1.4.1.5951.4.1.1.77.1.2 The address type of nsTdInetAddress

nsTdInetAddress

OID: 1.3.6.1.4.1.5951.4.1.1.77.1.3 This represents an IPv4/v6 address configured on the Citrix ADC

nsTdInetMaskLength

OID: 1.3.6.1.4.1.5951.4.1.1.77.1.4 This represents netmask length.

nsTdInetType

OID: 1.3.6.1.4.1.5951.4.1.1.77.1.5 This represents the IP address type

nsTdInetMode

OID: 1.3.6.1.4.1.5951.4.1.1.77.1.6 This represents the IP address mode

nsTdInetFreePorts

OID: 1.3.6.1.4.1.5951.4.1.1.77.1.7 This represents the number of unused ports free on this IP

nsTdInetVlan

OID: 1.3.6.1.4.1.5951.4.1.1.77.1.8 The vlan to which this ip address is bound.

nsTdInetBridgeGroup

OID: 1.3.6.1.4.1.5951.4.1.1.77.1.9 The bridge group to which this ip address is bound.

nsTdInetVxlan

OID: 1.3.6.1.4.1.5951.4.1.1.77.1.10 The vxlan to which this ip address is bound.

nsLLDPConfigGroup

OID: 1.3.6.1.4.1.5951.4.1.1.80.1 This provides the lldp configuration information of system.

nsLLDPMessageTxInterval

OID: 1.3.6.1.4.1.5951.4.1.1.80.1.1 TIme interval at which lldp packets will be sent.

nsLLDPMessageTxHoldMultiplier

OID: 1.3.6.1.4.1.5951.4.1.1.80.1.2 The time-to-live value expressed as a multiple of the lldpMessageTxInterval and lldpMessageTxHoldMultiplier.

nsLLDPStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.80.2 This provides statistics of LLDP traffic.

nsLLDPStatsTxPortTable

OID: 1.3.6.1.4.1.5951.4.1.1.80.2.1 This table contains information about statistics of LLDP packets transmission. This is indexed on the nsLLDPStatsTxPortNum.

nsLLDPStatsTxPortNum

OID: 1.3.6.1.4.1.5951.4.1.1.80.2.1.1.1 Interface number

nsLLDPStatsTxPortFramesTotal

OID: 1.3.6.1.4.1.5951.4.1.1.80.2.1.1.2 Total LLDP Packets transmitted

nsLLDPStatsRxPortTable

OID: 1.3.6.1.4.1.5951.4.1.1.80.2.2 This table contains information about statistics of recieved LLDP packets. This is indexed on the nsLLDPStatsRxPortNum.

nsLLDPStatsRxPortNum

OID: 1.3.6.1.4.1.5951.4.1.1.80.2.2.1.1 Interface number

nsLLDPStatsRxPortTLVsDiscardedTotal

OID: 1.3.6.1.4.1.5951.4.1.1.80.2.2.1.2 Total discarded LLDP packets.

nsLLDPStatsRxPortFramesErrors

OID: 1.3.6.1.4.1.5951.4.1.1.80.2.2.1.3 Total errors in LLDP packets.

nsLLDPStatsRxPortFramesTotal

OID: 1.3.6.1.4.1.5951.4.1.1.80.2.2.1.4 Total LLDP Packets received.

nsLLDPStatsRxPortTLVsUnrecognizedTotal

OID: 1.3.6.1.4.1.5951.4.1.1.80.2.2.1.5 Total TLVs not Recognised.

nsLLDPStatsRemTablesLastChangeTime

OID: 1.3.6.1.4.1.5951.4.1.1.80.2.3 Time stamp at which last change in Remote table seen.

nsLLDPStatsRemTablesInserts

OID: 1.3.6.1.4.1.5951.4.1.1.80.2.4 Total inserts in Remote LLDP table.

nsLLDPStatsRemTablesDeletes

OID: 1.3.6.1.4.1.5951.4.1.1.80.2.5 Total deletes in Remote LLDP table.

nsLLDPStatsRemTablesAgeouts

OID: 1.3.6.1.4.1.5951.4.1.1.80.2.6 Total Aged out entries in Remote LLDP table.

nsLLDPLocSystemsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.80.3 This provides LLDP info of local system.

nsLLDPLocPortTable

OID: 1.3.6.1.4.1.5951.4.1.1.80.3.1 This Table contains LLDP information of local port. This is indexed on the nsLLDPLocPortNum.

nsLLDPLocPortNum

OID: 1.3.6.1.4.1.5951.4.1.1.80.3.1.1.1 Interface Number

nsLLDPLocPortIdSubtype

OID: 1.3.6.1.4.1.5951.4.1.1.80.3.1.1.2 Local port id sub type

nsLLDPLocPortId

OID: 1.3.6.1.4.1.5951.4.1.1.80.3.1.1.3 Local port id

nsLLDPLocManAddrTable

OID: 1.3.6.1.4.1.5951.4.1.1.80.3.2 This Table contains LLDP information of local management address. This is indexed on the nsLLDPLocManAddrSubtype .

nsLLDPLocManAddrSubtype

OID: 1.3.6.1.4.1.5951.4.1.1.80.3.2.1.1 Management address subtype of Remote System

nsLLDPLocManAddr

OID: 1.3.6.1.4.1.5951.4.1.1.80.3.2.1.2 Management address of Local System

nsLLDPLocManAddrIfSubtype

OID: 1.3.6.1.4.1.5951.4.1.1.80.3.2.1.3 Interface subtype

nsLLDPLocManAddrIfId

OID: 1.3.6.1.4.1.5951.4.1.1.80.3.2.1.4 interface id

nsLLDPLocManAddrOID

OID: 1.3.6.1.4.1.5951.4.1.1.80.3.2.1.5 Management address OID

nsLLDPLocChassisIdSubtype

OID: 1.3.6.1.4.1.5951.4.1.1.80.3.3 Local chassis Id type

nsLLDPLocChassisId

OID: 1.3.6.1.4.1.5951.4.1.1.80.3.4 Local chassis Id

nsLLDPLocSysName

OID: 1.3.6.1.4.1.5951.4.1.1.80.3.5 Local Sytem Name

nsLLDPLocSysDesc

OID: 1.3.6.1.4.1.5951.4.1.1.80.3.6 Sytem description

nsLLDPLocSysCapSupported

OID: 1.3.6.1.4.1.5951.4.1.1.80.3.7 Capabilities supported by local system

nsLLDPLocSysCapEnabled

OID: 1.3.6.1.4.1.5951.4.1.1.80.3.8 Capabilities enabled on local system

nsLLDPRemTable

OID: 1.3.6.1.4.1.5951.4.1.1.80.4.1 This table contains lldp information of neighbors. This is indexed on the nsLLDPRemLocalPortNum.

nsLLDPRemTimeMark

OID: 1.3.6.1.4.1.5951.4.1.1.80.4.1.1.1 Time mark when lldp info recieved

nsLLDPRemLocalPortNum

OID: 1.3.6.1.4.1.5951.4.1.1.80.4.1.1.2 local nic no

nsLLDPRemChassisIdSubtype

OID: 1.3.6.1.4.1.5951.4.1.1.80.4.1.1.3 ChassisId subtype of remote system

nsLLDPRemChassisId

OID: 1.3.6.1.4.1.5951.4.1.1.80.4.1.1.4 Chassiss id of remote system

nsLLDPRemPortIdSubtype

OID: 1.3.6.1.4.1.5951.4.1.1.80.4.1.1.5 port id subtype of remote system

nsLLDPRemPortId

OID: 1.3.6.1.4.1.5951.4.1.1.80.4.1.1.6 port id of remote system

nsLLDPRemPortDesc

OID: 1.3.6.1.4.1.5951.4.1.1.80.4.1.1.7 port description of remote system

nsLLDPRemSysName

OID: 1.3.6.1.4.1.5951.4.1.1.80.4.1.1.8 remote system name

nsLLDPRemSysDesc

OID: 1.3.6.1.4.1.5951.4.1.1.80.4.1.1.9 remote system description

nsLLDPRemSysCapSupported

OID: 1.3.6.1.4.1.5951.4.1.1.80.4.1.1.10 remote system capabilities

nsLLDPRemSysCapEnabled

OID: 1.3.6.1.4.1.5951.4.1.1.80.4.1.1.11 enabled capabilities of system

nsLLDPRemManAddrTable

OID: 1.3.6.1.4.1.5951.4.1.1.80.4.2 This table contains LLDP information about management address of neighbors. This is indexed on the nsLLDPRemLocalPortNum and nsLLDPRemManAddr.

nsLLDPRemManAddrSubtype

OID: 1.3.6.1.4.1.5951.4.1.1.80.4.2.1.1 Management address subtype of Remote System

nsLLDPRemManAddr

OID: 1.3.6.1.4.1.5951.4.1.1.80.4.2.1.2 Management address of Remote System

nsLLDPRemManAddrIfSubtype

OID: 1.3.6.1.4.1.5951.4.1.1.80.4.2.1.3 Interface subtype

nsLLDPRemManAddrIfId

OID: 1.3.6.1.4.1.5951.4.1.1.80.4.2.1.4 interface id

nsLLDPRemManAddrOID

OID: 1.3.6.1.4.1.5951.4.1.1.80.4.2.1.5 Management address OID

vxlanTable

OID: 1.3.6.1.4.1.5951.4.1.1.81 The vxlan related statistics table. This is indexed on the vxlanVNId .

vxlanVNId

OID: 1.3.6.1.4.1.5951.4.1.1.81.1.1 This represents the VNID of the vxlan

vxlanTotRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.81.1.2 Packets received on the VXLAN.

vxlanTotRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.81.1.3 Bytes of data received on the VXLAN.

vxlanTotTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.81.1.4 Packets transmitted on the VXLAN.

vxlanTotTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.81.1.5 Bytes of data transmitted on the VXLAN.

cacheGroupTable

OID: 1.3.6.1.4.1.5951.4.1.1.82 Content Group Table This is indexed on the cachegroupName .

cachegroupName

OID: 1.3.6.1.4.1.5951.4.1.1.82.1.1 Encoded name of the cache group

groupnon304hit

OID: 1.3.6.1.4.1.5951.4.1.1.82.1.2 Non304 hits for ContentGroup

group304hit

OID: 1.3.6.1.4.1.5951.4.1.1.82.1.3 304 hits for ContentGroup

totcell

OID: 1.3.6.1.4.1.5951.4.1.1.82.1.4 Number of objects in contentgroup

totmarkercell

OID: 1.3.6.1.4.1.5951.4.1.1.82.1.5 Number of marker objects in contentgroup

timesflushed

OID: 1.3.6.1.4.1.5951.4.1.1.82.1.6 Number of times contentgroup is flushed

totmemory

OID: 1.3.6.1.4.1.5951.4.1.1.82.1.7 current memory usage

maxmemory

OID: 1.3.6.1.4.1.5951.4.1.1.82.1.8 maximum memory usage limit

nsLsnGlobalStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.83.1 This provides statistics for LSN

lsnTotRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.1 Current number of LSN rx pkts.

lsnTotRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.2 Current number of LSN rx bytes.

lsnTotTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.3 Current number of LSN tx pkts.

lsnTotTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.4 Current number of LSN tx bytess.

lsnCurSessions

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.5 Current number of LSN sessions.

lsnCurSubscribers

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.6 Current number of LSN subscribers.

lsnTotTcpRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.7 Number of LSN TCP Received packets.

lsnTotTcpTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.8 Number of LSN TCP Transmitted packets.

lsnTotUdpRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.9 Number of LSN UDP Received packets.

lsnTotUdpTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.10 Number of LSN UDP Transmitted packets.

lsnTotIcmpRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.11 Number of LSN ICMP Received packets.

lsnTotIcmpTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.12 Number of LSN ICMP Transmitted packets.

lsnTotTcpRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.13 Number of LSN TCP Received bytes.

lsnTotTcpTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.14 Number of LSN TCP Transmitted bytes.

lsnTotUdpRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.15 Number of LSN UDP Received bytes.

lsnTotUdpTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.16 Number of LSN UDP Transmitted bytes.

lsnTotIcmpRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.17 Number of LSN ICMP Received bytes.

lsnTotIcmpTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.18 Number of LSN ICMP Transmitted bytes.

lsnTotDrpPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.19 Tot number of LSN Dropped packets.

lsnTotTcpDrpPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.20 Number of LSN TCP Dropped packets.

lsnTotUdpDrpPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.21 Number of LSN UDP Dropped packets.

lsnTotIcmpDrpPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.22 Number of LSN ICMP Dropped packets.

lsnCurTcpSessions

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.23 Number of LSN TCP Current Sessions.

lsnCurUdpSessions

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.24 Number of LSN UDP Current Sessions.

lsnCurIcmpSessions

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.25 Number of LSN ICMP Current Sessions.

lsnSessionsRate

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.26 Rate at which total LSN sessions are opened per second.

lsnTcpSessionsRate

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.27 Rate at which total LSN sessions are opened per second.

lsnUdpSessionsRate

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.28 Rate at which total LSN sessions are opened per second.

lsnIcmpSessionsRate

OID: 1.3.6.1.4.1.5951.4.1.1.83.1.29 Rate at which total LSN sessions are opened per second.

nsLsnGroupTable

OID: 1.3.6.1.4.1.5951.4.1.1.83.2 This table contains statistics related to LSN group This is indexed on the lsnGrpName .

lsnGrpName

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.1 The name of the LSN Group

lsnGrpTotTranslPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.2 Number of Translated Pkts for LSN group

lsnGrpTotTranslBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.3 Number of Translated Bytes for LSN group

lsnGrpCurSessions

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.4 Number of Current Sessions for LSN group

lsnGrpCurSubscribers

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.5 Number of ICMP Current Sessions for LSN group

lsnGrpTotTcpTranslPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.6 Number of TCP Translated Pkts for LSN group

lsnGrpTotUdpTranslPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.7 Number of UDP Translated Pkts for LSN group

lsnGrpTotIcmpTranslPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.8 Number of ICMP Translated Pkts for LSN group

lsnGrpTotTcpTranslBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.9 Number of TCP Translated Bytes for LSN group

lsnGrpTotUdpTranslBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.10 Number of UDP Translated Bytes for LSN group

lsnGrpTotIcmpTranslBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.11 Number of ICMP Translated Bytes for LSN group

lsnGrpTotTcpDrpPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.12 Number of TCP Dropped Pkts for LSN group

lsnGrpTotUdpDrpPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.13 Number of UDP Dropped Pkts for LSN group

lsnGrpTotIcmpDrpPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.14 Number of ICMP Dropped Pkts for LSN group

lsnGrpTotTcpDrpBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.15 Number of TCP Dropped Bytes for LSN group

lsnGrpTotUdpDrpBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.16 Number of UDP Dropped Bytes for LSN group

lsnGrpTotIcmpDrpBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.17 Number of ICMP Dropped Bytes for LSN group

lsnGrpCurTcpSessions

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.18 Number of TCP Current Sessions for LSN group

lsnGrpCurUdpSessions

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.19 Number of UDP Current Sessions for LSN group

lsnGrpCurIcmpSessions

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.20 Number of ICMP Current Sessions for LSN group

lsnGrpSessRate

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.21 Rate at which LSN sessions of group are opened per second.

lsnGrpTcpSessRate

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.22 Rate at which LSN TCP sessions of group are opened per second.

lsnGrpUdpSessRate

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.23 Rate at which LSN UDP sessions of group are opened per second.

lsnGrpIcmpSessRate

OID: 1.3.6.1.4.1.5951.4.1.1.83.2.1.24 Rate at which LSN ICMP sessions of group are opened per second.

nsPPTPStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.83.3 This provides statistics related to PPTP.

pptpCurCtrlSessions

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.1 Total number of currrent PPTP control sessions.

pptpTotCtrlSessions

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.2 Total number of PPTP control sessions.

pptpTotGRESessions

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.3 Total number of PPTP GRE sessions.

pptpCurGRESessions

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.4 Total number of current PPTP GRE sessions.

pptpStrtCtrlConnReply

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.5 Number of PPTP start control connection replies.

pptpStpCtrlConnReply

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.6 Number of PPTP stop control connection replies.

pptpOutCallReply

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.7 Number of PPTP out call replies.

pptpCtlErrNoCallidMap

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.8 Number of PPTP control no callid map.

pptpInCallReq

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.9 Number of PPTP in call request.

pptpInCallConn

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.10 Number of PPTP in call connected.

pptpCallDisNotify

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.11 Number of PPTP call disconnect notification.

pptpWanErrNotify

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.12 Number of PPTP WAN Error notification.

pptpSetLinkInfo

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.13 Number of PPTP set link information.

pptpEchoReq

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.14 Number of PPTP echo request.

pptpEchoRep

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.15 Number of PPTP echo reply.

pptpStrtCtrlConnReq

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.16 Number of PPTP start Control Connection request.

pptpStpCtrlConnReq

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.17 Number of PPTP stop Control Connection request.

pptpOutCallReq

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.18 Number of PPTP out call request.

pptpInCallRep

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.19 Number of PPTP in call reply.

pptpCallClrReq

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.20 Number of PPTP call Clear request.

pptpCntlOcreq

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.21 Number of PPTP control ocreq error create callid map.

pptpCntlIcreq

OID: 1.3.6.1.4.1.5951.4.1.1.83.3.22 Number of PPTP icreq control error create callid map.

nsLsnDSLiteGlobalStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.83.4 This provides statistics for LSN DS-Lite

lsnTotDSLiteRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.4.1 Total number of LSN DS-Lite rx pkts.

lsnTotDSLiteRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.4.2 Total number of LSN DS-Lite rx bytes.

lsnTotDSLiteTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.4.3 Total number of LSN DS-Lite tx pkts.

lsnTotDSLiteTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.4.4 Total number of LSN DS-Lite tx bytes.

lsnCurDSLiteSessions

OID: 1.3.6.1.4.1.5951.4.1.1.83.4.5 Current number of LSN DS-Lite sessions.

lsnDSLiteCurSubscribers

OID: 1.3.6.1.4.1.5951.4.1.1.83.4.6 Current number of LSN DS-Lite subscribers.

nsLsnLogStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.83.5 This provides logging statistics for LSN

nsLsnMappingLogStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.1 This provides mapping log statistics for LSN

lsnLogTotMappingCreateEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.1.1 Total create-mapping entires logged.

lsnLogTotMappingDeleteEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.1.2 Total delete-mapping entires logged.

lsnLogTotAPDMappingCreateEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.1.3 Total create-mappings of addrport dependent logged.

lsnLogTotAPDMappingDeleteEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.1.4 Total no of delete-mappings of address port dependent type logged.

lsnLogTotADMappingCreateEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.1.5 Total create-mappings of Address dependent type logged.

lsnLogTotADMappingDeleteEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.1.6 Total no of delete-mappings of Address dependent type logged.

lsnLogTotEIMappingCreateEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.1.7 Total create-mappings of Endpoint-Independent type logged.

lsnLogTotEIMappingDeleteEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.1.8 Total no of delete-mappings of Endpoint Independent type logged.

lsnLogTotTcpMappingCreateEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.1.9 Total create-mappings for TCP logged.

lsnLogTotTcpMappingDeleteEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.1.10 Total delete-mappings for TCP logged.

lsnLogTotUdpMappingCreateEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.1.11 Total create-mappings for UDP logged.

lsnLogTotUdpMappingDeleteEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.1.12 Total delete-mappings for UDP logged.

lsnLogTotIcmpMappingCreateEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.1.13 Total create-mappings for ICMP logged.

lsnLogTotIcmpMappingDeleteEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.1.14 Total delete-mappings for ICMP logged.

lsnLogTotWrongMappingFlagEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.1.15 Total number of time wrong mapping-type was encountered while logging.

nsLsnSessionLogStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.2 This provides session log statistics for LSN

lsnLogTotSessionCreateEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.2.1 Total no of create-sessions logged.

lsnLogTotSessionDeleteEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.2.2 Total no of delete-sessions logged.

lsnLogTotTcpSessionCreateEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.2.3 Total create-sessions for TCP logged.

lsnLogTotTcpSessionDeleteEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.2.4 Total delete-sessions for TCP logged.

lsnLogTotUdpSessionCreateEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.2.5 Total create-sessions for UDP logged.

lsnLogTotUdpSessionDeleteEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.2.6 Total delete-sessions for UDP logged.

lsnLogTotIcmpSessionCreateEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.2.7 Total create-sessions for ICMP logged.

lsnLogTotIcmpSessionDeleteEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.2.8 Total delete-sessions for ICMP logged.

lsnLogTotEntries

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.3 Total session/mapping entries logged.

lsnLogTotDeterministicAllocs

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.4 Total deterministic NAT allocations logged.

lsnLogTotDeterministicDeallocs

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.5 Total determistic NAT deletions logged

lsnLogTotPortblockAllocs

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.6 Total portblock NAT allocations logged.

lsnLogTotPortblockDeallocs

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.7 Total portblock NAT deallocations logged.

lsnLogTotTcpPortblockAllocs

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.8 Total portblock NAT allocations for tcp logged.

lsnLogTotTcpPortblockDeallocs

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.9 Total portblock NAT deallocations for tcp logged.

lsnLogTotNontcpPortblockAllocs

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.10 Total portblock NAT allocations for udp and icmp logged.

lsnLogTotNontcpPortblockDeallocs

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.11 Total portblock NAT deallocations for udp and icmp logged.

lsnLogTotWrongFlags

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.12 Total no of times incorrect flag(neither create nor delete) encountered while logging.

lsnLogTotWrongProtocols

OID: 1.3.6.1.4.1.5951.4.1.1.83.5.13 Wrong protocol popped up in logentry.

nsLsnNAT64GlobalStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.83.6 This provides statistics for LSN NAT64

lsnTotNAT64RxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.1 Total number of LSN NAT64 rx pkts.

lsnTotNAT64RxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.2 Total number of LSN NAT64 rx bytes.

lsnTotNAT64TxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.3 Total number of LSN NAT64 tx pkts.

lsnTotNAT64TxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.4 Total number of LSN NAT64 tx bytes.

lsnCurNAT64sessions

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.5 Current number of LSN NAT64 sessions.

lsnNAT64CurSubscribers

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.6 Current number of LSN NAT64 subscribers.

lsnTotNAT64TcpRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.7 Number of LSN NAT64 TCP Received packets.

lsnTotNAT64TcpTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.8 Number of LSN NAT64 TCP Transmitted packets.

lsnTotNAT64UdpRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.9 Number of LSN NAT64 UDP Received packets.

lsnTotNAT64UdpTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.10 Number of LSN NAT64 UDP Transmitted packets.

lsnTotNAT64IcmpRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.11 Number of LSN NAT64 ICMP Received packets.

lsnTotNAT64IcmpTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.12 Number of LSN NAT64 ICMP Transmitted packets.

lsnTotNAT64TcpRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.13 Number of LSN NAT64 TCP Received bytes.

lsnTotNAT64TcpTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.14 Number of LSN NAT64 TCP Transmitted bytes.

lsnTotNAT64UdpRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.15 Number of LSN NAT64 UDP Received bytes.

lsnTotNAT64UdpTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.16 Number of LSN NAT64 UDP Transmitted bytes.

lsnTotNAT64IcmpRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.17 Number of LSN NAT64 ICMP Received bytes.

lsnTotNAT64IcmpTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.18 Number of LSN NAT64 ICMP Transmitted bytes.

lsnTotNAT64TcpDrpPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.19 Number of LSN NAT64 TCP Dropped packets.

lsnTotNAT64UdpDrpPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.20 Number of LSN NAT64 UDP Dropped packets.

lsnTotnat64IcmpDrpPkts

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.21 Number of LSN NAT64 ICMP Dropped packets.

lsnCurNAT64TcpSessions

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.22 Number of LSN NAT64 TCP Current Sessions.

lsnCurNAT64UdpSessions

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.23 Number of LSN NAT64 UDP Current Sessions.

lsnCurNAT64IcmpSessions

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.24 Number of LSN NAT64 ICMP Current Sessions.

lsnNAT64SessionsRate

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.25 Rate at which total LSN NAT64 sessions are opened per second.

lsnNAT64TcpSessionsRate

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.26 Rate at which total LSN NAT64 sessions are opened per second.

lsnNAT64UdpSessionsRate

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.27 Rate at which total LSN NAT64 sessions are opened per second.

lsnNAT64IcmpSessionsRate

OID: 1.3.6.1.4.1.5951.4.1.1.83.6.28 Rate at which total LSN sessions are opened per second.

nsLsnPoolTable

OID: 1.3.6.1.4.1.5951.4.1.1.83.7 This table contains statistics related to LSN pool This is indexed on the lsnPoolName .

lsnPoolName

OID: 1.3.6.1.4.1.5951.4.1.1.83.7.1.1 The name of the LSN Pool

lsnpoolTotIps

OID: 1.3.6.1.4.1.5951.4.1.1.83.7.1.2 Total IPs in this pool.

lsnpoolCurPortAllocTcp

OID: 1.3.6.1.4.1.5951.4.1.1.83.7.1.3 Current port allocation for tcp in this pool.

lsnpoolCurPortAllocOther

OID: 1.3.6.1.4.1.5951.4.1.1.83.7.1.4 Current port allocation for other protocols in this pool.

lsnpoolTcpPortUsagePercen

OID: 1.3.6.1.4.1.5951.4.1.1.83.7.1.5 TCP ports usage percentage in this pool.

lsnpoolOtherPortUsagePercen

OID: 1.3.6.1.4.1.5951.4.1.1.83.7.1.6 Other protocols ports usage percentage in this pool.

nsmcStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.84 This provides information about Media classification related statistics in the Netscaler product.

mcTotaudio

OID: 1.3.6.1.4.1.5951.4.1.1.84.1

mcTotvideo

OID: 1.3.6.1.4.1.5951.4.1.1.84.2

mcTotother

OID: 1.3.6.1.4.1.5951.4.1.1.84.3

mcMsSmthStrmVid

OID: 1.3.6.1.4.1.5951.4.1.1.84.4 This tells the total number of Microsoft SmoothStreaming videos served by NS

mcMsSmthStrmVidBytes

OID: 1.3.6.1.4.1.5951.4.1.1.84.5 This tells the total number of Microsoft SmoothStreaming video bytes served by NS

mcMsSmthStrVidpl

OID: 1.3.6.1.4.1.5951.4.1.1.84.6 This tells the total number of Microsoft SmoothStreaming playlist served by NS

mcMsSmthStrmPlVidBytespl

OID: 1.3.6.1.4.1.5951.4.1.1.84.7 This tells the total number of Microsoft SmoothStreaming playlist bytes served by NS

mccApleLiveStrmngVid

OID: 1.3.6.1.4.1.5951.4.1.1.84.8 This tells the total number of AppleLive videos served by NS

mcAppleLiveStreamingVidBytes

OID: 1.3.6.1.4.1.5951.4.1.1.84.9 This tells the total number of AppleLive video bytes served by NS

mccAppleLiveStrmngVidpl

OID: 1.3.6.1.4.1.5951.4.1.1.84.10 This tells the total number of AppleLive Playlist served by NS

mcAppleLiveStreamingPlaylistVidBytespl

OID: 1.3.6.1.4.1.5951.4.1.1.84.11 This tells the total number of AppleLive Playlist bytes served by NS

mcADTSaudio

OID: 1.3.6.1.4.1.5951.4.1.1.84.12 This tells the total number of ADTS audios served by NS

mcADTSaudioBytes

OID: 1.3.6.1.4.1.5951.4.1.1.84.13 This tells the total number of ADTS audio bytes served by NS

mcAACaudio

OID: 1.3.6.1.4.1.5951.4.1.1.84.14 This tells the total number of AAC audios served by NS

mcAACaudiobytes

OID: 1.3.6.1.4.1.5951.4.1.1.84.15 This tells the total number of AAC bytes served by NS

mcFLVVid

OID: 1.3.6.1.4.1.5951.4.1.1.84.16 This tells the total number of FLV videos served by NS

mcFLVVidBytes

OID: 1.3.6.1.4.1.5951.4.1.1.84.17 This tells the total number of FLV bytes served by NS

mcMP4Vid

OID: 1.3.6.1.4.1.5951.4.1.1.84.18 This tells the total number of MP4 videos served by NS

mcMP4VidBytes

OID: 1.3.6.1.4.1.5951.4.1.1.84.19 This tells the total number of MP4 video bytes served by NS

mc3PVid

OID: 1.3.6.1.4.1.5951.4.1.1.84.20 This tells the total number of 3GP videos served by NS

mc3GPVidBytes

OID: 1.3.6.1.4.1.5951.4.1.1.84.21 This tells the total number of 3GP bytes served by NS

mcTotResponse

OID: 1.3.6.1.4.1.5951.4.1.1.84.22

mcAndroid

OID: 1.3.6.1.4.1.5951.4.1.1.84.23 Total number of android requests to Citrix ADC

mcLaptopDesktp

OID: 1.3.6.1.4.1.5951.4.1.1.84.24 Total number of laptop/desktop requests to Citrix ADC

mcIos

OID: 1.3.6.1.4.1.5951.4.1.1.84.25 Total number of IOS requests to Citrix ADC

mcUnidentified

OID: 1.3.6.1.4.1.5951.4.1.1.84.26 Total number of unidentified requests to Citrix ADC

mcOther

OID: 1.3.6.1.4.1.5951.4.1.1.84.27 Total number of other mobile device requests to Citrix ADC

mcYoutubedash

OID: 1.3.6.1.4.1.5951.4.1.1.84.28 This tells the total number of YouTube DASH served by NS

mcYoutubedashBytes

OID: 1.3.6.1.4.1.5951.4.1.1.84.29 This tells the total number of YouTube DASH bytes served by NS

mcEncVideo

OID: 1.3.6.1.4.1.5951.4.1.1.84.30 Total number of encrypted video streams

mcEncHls

OID: 1.3.6.1.4.1.5951.4.1.1.84.31 Total number of encrypted AppleLive video streams

mcEncDASH

OID: 1.3.6.1.4.1.5951.4.1.1.84.32 Total number of encrypted Youtube DASH video streams

mcEncOthStream

OID: 1.3.6.1.4.1.5951.4.1.1.84.33 Total number of non-AppleLive, non-DASH encrypted streams

mcEncAndroid

OID: 1.3.6.1.4.1.5951.4.1.1.84.34 Total number of encrypted video streams requested by Android devices

mcEncIos

OID: 1.3.6.1.4.1.5951.4.1.1.84.35 Total number of encrypted video streams requested by IOS devices

mcEncOther

OID: 1.3.6.1.4.1.5951.4.1.1.84.36 Total number of encrypted video streams requested by non-Android and non-IOS devices

nsMapDomainStatsTable

OID: 1.3.6.1.4.1.5951.4.1.1.85.1 This provides information about MAP-T domain specific statistics This is indexed on the mapDomainName .

mapDomainName

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.1 The name of the LSN Group

mapTotV6RxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.2 Total number of MAP-T V6 Recieved packets.

mapTotV6TxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.3 Total number of MAP-T V6 Transmitted packets.

mapTotV6RxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.4 Total number of MAP-T V6 Recieved Bytes.

mapTotV6TxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.5 Total number of MAP-T V6 Transmitted Bytes.

mapTotV4RxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.6 Total number of MAP-T V4 Recieved packets.

mapTotV4TxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.7 Total number of MAP-T V4 Transmitted packets.

mapTotV4RxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.8 Total number of MAP-T V4 Recieved Bytes.

mapTotV4TxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.9 Total number of MAP-T V4 Transmitted Bytes.

mapTotV6RxPktsTcp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.10 Total number of MAP-T IPv6 TCP Recieved packets.

mapTotV6TxPktsTcp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.11 Total number of MAP-T IPv6 TCP Transmitted packets.

mapTotV6RxBytesTcp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.12 Total number of MAP-T IPv6 TCP Recieved Bytes.

mapTotV6TxBytesTcp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.13 Total number of MAP-T IPv6 TCP Transmitted Bytes.

mapTotV4RxPktsTcp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.14 Total number of MAP-T IPv4 TCP Recieved packets.

mapTotV4TxPktsTcp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.15 Total number of MAP-T IPv4 TCP Transmitted packets.

mapTotV4RxBytesTcp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.16 Total number of MAP-T IPv4 TCP Recieved Bytes.

mapTotV4TxBytesTcp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.17 Total number of MAP-T IPv4 TCP Transmitted Bytes.

mapTotV6RxPktsUdp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.18 Total number of MAP-T IPv6 UDP Recieved packets.

mapTotV6TxPktsUdp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.19 Total number of MAP-T IPv6 UDP Transmitted packets.

mapTotV6RxBytesUdp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.20 Total number of MAP-T IPv6 UDP Recieved Bytes.

mapTotV6TxBytesUdp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.21 Total number of MAP-T IPv6 UDP Transmitted Bytes.

mapTotV4RxPktsUdp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.22 Total number of MAP-T IPv4 UDP Recieved packets.

mapTotV4TxPktsUdp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.23 Total number of MAP-T IPv4 UDP Transmitted packets.

mapTotV4RxBytesUdp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.24 Total number of MAP-T IPv4 UDP Recieved Bytes.

mapTotV4TxBytesUdp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.25 Total number of MAP-T IPv4 UDP Transmitted Bytes.

mapTotV6RxPktsIcmp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.26 Total number of MAP-T IPv6 ICMP Recieved packets.

mapTotV6TxPktsIcmp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.27 Total number of MAP-T IPv6 ICMP Transmitted packets.

mapTotV6RxBytesIcmp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.28 Total number of MAP-T IPv6 ICMP Recieved Bytes.

mapTotV6TxBytesIcmp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.29 Total number of MAP-T IPv6 ICMP Transmitted Bytes.

mapTotV4RxPktsIcmp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.30 Total number of MAP-T IPv4 ICMP Recieved packets.

mapTotV4TxPktsIcmp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.31 Total number of MAP-T IPv4 ICMP Transmitted packets.

mapTotV4RxBytesIcmp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.32 Total number of MAP-T IPv4 ICMP Recieved Bytes.

mapTotV4TxBytesIcmp

OID: 1.3.6.1.4.1.5951.4.1.1.85.1.1.33 Total number of MAP-T IPv4 ICMP Transmitted Bytes.

nsIpSecAlgProfTable

OID: 1.3.6.1.4.1.5951.4.1.1.86 This table contains IPSec ALG information about seesions of the profile. This is indexed on the ipSecAlgProfName.

ipSecAlgProfName

OID: 1.3.6.1.4.1.5951.4.1.1.86.1.1 The name of the IPSec ALG Profile

ipSecAlgTotSessions

OID: 1.3.6.1.4.1.5951.4.1.1.86.1.2 Total session for IPSec ALG.

ipSecAlgTotDrSessions

OID: 1.3.6.1.4.1.5951.4.1.1.86.1.3 Total Dropped IPsec ALG sessions.

ipSecAlgCurActSessions

OID: 1.3.6.1.4.1.5951.4.1.1.86.1.4 Currently active IPsec ALG sessions.

ipSecAlgCurBlkSessions

OID: 1.3.6.1.4.1.5951.4.1.1.86.1.5 Currently blocked sessions on ESP Gate.

ipSecAlgTotRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.86.1.6 Total Packets received during IPsec ALG sessions.

ipSecAlgTotTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.86.1.7 Total Packets sent during IPsec ALG sessions.

nsRnat6GlobalStats

OID: 1.3.6.1.4.1.5951.4.1.1.87.1 This provides statistics related to all RNAT6 sessions.

rnat6TotRxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.87.1.1 Bytes received during RNAT6 sessions.

rnat6TotTxBytes

OID: 1.3.6.1.4.1.5951.4.1.1.87.1.2 Bytes sent during RNAT6 sessions.

rnat6TotRxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.87.1.3 Packets received during RNAT6 sessions.

rnat6TotTxPkts

OID: 1.3.6.1.4.1.5951.4.1.1.87.1.4 Packets sent during RNAT6 sessions.

rnat6TotTxSyn

OID: 1.3.6.1.4.1.5951.4.1.1.87.1.5 Requests for connections sent during RNAT6 sessions.

rnat6CurSessions

OID: 1.3.6.1.4.1.5951.4.1.1.87.1.6 Currently active RNAT6 sessions.

partitionTable

OID: 1.3.6.1.4.1.5951.4.1.1.88 Admin partition related statistics table. This is indexed on the partitionName .

partitionName

OID: 1.3.6.1.4.1.5951.4.1.1.88.1.1 This is the partition name

partitionCurrentBandwidth

OID: 1.3.6.1.4.1.5951.4.1.1.88.1.2 Current Bandwidth usage for the partition.

partitionCurrentConnections

OID: 1.3.6.1.4.1.5951.4.1.1.88.1.3 Current Connections on this partition.

partitionMemoryUsagePcnt

OID: 1.3.6.1.4.1.5951.4.1.1.88.1.4 Memory usage(%) on this partition.

botManagementStatistics

OID: 1.3.6.1.4.1.5951.4.1.1.89.1 This provides Bot Management statistics in the Netscaler product.

botRequests

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.1 HTTP/HTTPS requests sent to your protected web servers via the Bot Management.

botResponses

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.2 HTTP/HTTPS responses sent by your protected web servers via the Bot Management.

botReqBytes

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.3 Number of bytes transfered for requests

botResBytes

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.4 Number of bytes transfered for responses

botViolDeviceFingerPrint

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.5 Number of device fingerprint violations seen by the Bot Management.

botViolDeviceFingerPrintLog

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.6 Number of device fingerprint violations logged by the Bot Management.

botViolDeviceFingerPrintDrop

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.7 Number of device fingerprint violations dropped by the Bot Management.

botViolDeviceFingerPrintRedirect

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.8 Number of device fingerprint violations requests redirected by the Bot Management to a different Web page or web server.

botViolIPReputation

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.9 Number of ip reputation violations seen by the Bot Management.

botViolIPReputationLog

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.10 Number of ip reputation violations logged by the Bot Management.

botViolIPReputationDrop

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.11 Number of ip reputation violations dropped by the Bot Management.

botViolIPReputationRedirect

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.12 Number of ip reputation violations requests redirected by the Bot Management to a different Web page or web server.

botViolWhiteList

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.13 Number of white list violations seen by the Bot Management.

botViolWhiteListLog

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.14 Number of white list violations logged by the Bot Management.

botViolBlackList

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.15 Number of black list violations seen by the Bot Management.

botViolBlackListLog

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.16 Number of black list violations logged by the Bot Management.

botViolBlackListDrop

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.17 Number of black list violations dropped by the Bot Management.

botViolBlackListRedirect

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.18 Number of black list violations redirected by the Bot Management to a different Web page or web server.

botViolRateLimit

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.19 Number of rate limiting violations seen by the Bot Management.

botViolRateLimitLog

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.20 Number of rate limiting violations logged by the Bot Management.

botViolRateLimitDrop

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.21 Number of rate limiting violations dropped by the Bot Management.

botViolRateLimitRedirect

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.22 Number of rate limiting violations requests redirected by the Bot Management to a different Web page or web server.

botViolStaticSignature

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.23 Number of static signature violations seen by the Bot Management.

botViolStaticSignatureLog

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.24 Number of static signature violations logged by the Bot Management.

botViolStaticSignatureDrop

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.25 Number of static signature violations dropped by the Bot Management.

botViolStaticSignatureRedirect

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.26 Number of static signature violations requests redirected by the Bot Management to a different Web page or web server.

botViolDeviceFingerPrintCaptcha

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.27 Number of device fingerprint violations requests for which CAPTCHA challenge was sent.

botViolIPReputationCaptcha

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.28 Number of ip reputation violations requests for which CAPTCHA challenge was sent.

botViolStaticSignatureReset

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.29 Number of static signature violations requests reset by the Bot Management to a different Web page or web server.

botViolTps

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.30 Number of tps violations seen by the Bot Management.

botViolTpsLog

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.31 Number of tps violations logged by the Bot Management.

botViolTpsDrop

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.32 Number of tps violations dropped by the Bot Management.

botViolTpsRedirect

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.33 Number of tps violations requests redirected by the Bot Management to a different Web page or web server.

botViolTpsReset

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.34 Number of tps violations reset by the Bot Management.

botViolTpsCaptcha

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.35 Number of TPS violations requests for which CAPTCHA challenge was sent.

botViolDeviceFingerPrintReset

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.36 Number of device fingerprint violations reset by the Bot Management.

botViolIPReputationReset

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.37 Number of ip reputation violations reset by the Bot Management.

botViolBlackListReset

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.38 Number of black list violations reset by the Bot Management.

botViolRateLimitReset

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.39 Number of rate limiting violations reset by the Bot Management.

botViolCaptchaReset

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.40 Number of Captcha challenge failures reset by the Bot Management.

botViolCaptcha

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.41 Number of Captcha challenge failures seen by the Bot Management.

botViolCaptchaLog

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.42 Number of Captcha challenge failures logged by the Bot Management.

botViolCaptchaDrop

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.43 Number of Captcha challenge failures dropped by the Bot Management.

botViolCaptchaRedirect

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.44 Number of Captcha challenge failures redirected by the Bot Management.

botViolTrap

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.45 Number of trap violations seen by the Bot Management.

botViolTrapLog

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.46 Number of trap violations logged by the Bot Management.

botViolTrapDrop

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.47 Number of trap violations dropped by the Bot Management.

botViolTrapRedirect

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.48 Number of trap violations requests redirected by the Bot Management to a different Web page or web server.

botViolTrapReset

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.49 Number of trap violations reset by the Bot Management.

botViolRateLimitExceededResponse

OID: 1.3.6.1.4.1.5951.4.1.1.89.1.50 Number of rate limiting violations requests resulted in too many requests response by the Bot Management.

botProfileTable

OID: 1.3.6.1.4.1.5951.4.1.1.89.2

This is indexed on the appfwprofileName.

botBotRequestsPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.1 HTTP/HTTPS requests sent to your protected web servers via the Bot profile.

botBotResponsesPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.2 HTTP/HTTPS responses sent by your protected web servers via the Bot profile.

botBotReqBytesPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.3 Number of bytes transfered for requests

botBotResBytesPerProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.4 Number of bytes transfered for responses

botBotViolDeviceFingerPrintProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.5 Number of device fingerprint violations seen by the Bot profile.

botBotViolDeviceFingerPrintLogProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.6 Number of device fingerprint violations logged by the Bot profile.

botBotViolDeviceFingerPrintDropProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.7 Number of device fingerprint violations dropped by the Bot profile.

botBotViolDeviceFingerPrintRedirectProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.8 Number of device fingerprint violations requests redirected by the Bot profile to a different Web page or web server.

botBotViolIPReputationProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.9 Number of ip reputation violations seen by the Bot profile.

botBotViolIPReputationLogProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.10 Number of ip reputation violations logged by the Bot Profile.

botBotViolIPReputationDropProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.11 Number of ip reputation violations dropped by the Bot profile.

botBotViolIPReputationRedirectProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.12 Number of ip reputation violations requests redirected by the Bot profile to a different Web page or web server.

botBotViolWhiteListProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.13 Number of white list violations seen by the Bot profile.

botBotViolWhiteListLogProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.14 Number of white list violations logged by the Bot profile.

botBotViolBlackListProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.15 Number of black list violations seen by the Bot profile.

botBotViolBlackListLogProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.16 Number of black list violations logged by the Bot profile.

botBotViolBlackListDropProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.17 Number of black list violations dropped by the Bot profile.

botBotViolBlackListRedirectProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.18 Number of black list violations redirected by the Bot profile to a different Web page or web server.

botBotViolRateLimitProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.19 Number of rate limiting violations seen by the Bot profile.

botBotViolRateLimitLogProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.20 Number of rate limiting violations logged by the Bot profile.

botBotViolRateLimitDropProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.21 Number of rate limiting violations dropped by the Bot profile.

botBotViolRateLimitRedirectProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.22 Number of rate limiting violations requests redirected by the Bot profile to a different Web page or web server.

botBotViolStaticSignatureProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.23 Number of static signatutre violations seen by the Bot profile.

botBotViolStaticSignatureLogProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.24 Number of static signatutre violations logged by the Bot profile.

botBotViolStaticSignatureDropProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.25 Number of static signatutre violations dropped by the Bot profile.

botBotViolStaticSignatureRedirectProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.26 Number of static signatutre violations redirected by the Bot profile to a different Web page or web server.

botBotViolDeviceFingerPrintCaptchaProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.27 Number of device fingerprint violation requests for which CAPTCHA challenge was sent due to Bot profile.

botBotViolIPReputationCaptchaProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.28 Number of ip reputation violation requests for which CAPTCHA challenge was sent due to Bot profile.

botBotViolStaticSignatureResetProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.29 Number of static signatutre violations reset by the Bot profile to a different Web page or web server.

botBotViolTpsProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.30 Number of tps violations seen by the Bot profile.

botBotViolTpsLogProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.31 Number of tps violations logged by the Bot profile.

botBotViolTpsDropProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.32 Number of tps violations dropped by the Bot profile.

botBotViolTpsRedirectProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.33 Number of tps violations requests redirected by the Bot profile to a different Web page or web server.

botBotViolTpsResetProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.34 Number of tps violations reset by the Bot profile.

botBotViolTpsCaptchaProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.35 Number of tps violation requests for which CAPTCHA challenge was sent due to Bot profile.

botBotViolDeviceFingerPrintResetProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.36 Number of device fingerprint violations reset by the Bot profile.

botBotViolIPReputationResetProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.37 Number of ip reputation violations reset by the Bot profile.

botBotViolBlackListResetProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.38 Number of black list violations reset by the Bot profile.

botBotViolRateLimitResetProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.39 Number of rate limiting violations reset by the Bot profile.

botBotViolCaptchaResetProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.40 Number of Captcha challenge failures reset by the Bot profile.

botBotViolCaptchaProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.41 Number of Captcha challenge failures seen by the Bot profile.

botBotViolCaptchaLogProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.42 Number of Captcha challenge failures logged by the Bot profile.

botBotViolCaptchaDropProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.43 Number of Captcha challenge failures dropped by the Bot profile.

botBotViolCaptchaRedirectProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.44 Number of Captcha challenge failures redirected by the Bot profile.

botBotViolTrapProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.45 Number of trap violations seen by the Bot profile.

botBotViolTrapLogProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.46 Number of trap violations logged by the Bot profile.

botBotViolTrapDropProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.47 Number of trap violations dropped by the Bot profile.

botBotViolTrapRedirectProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.48 Number of trap violations requests redirected by the Bot profile to a different Web page or web server.

botBotViolTrapResetProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.49 Number of trap violations reset by the Bot profile.

botbotViolRateLimitExceededResponseProfile

OID: 1.3.6.1.4.1.5951.4.1.1.89.2.1.50 Number of rate limiting violations requests responded resulted in too many requests response by the Bot profile.

nsHttp2StatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.90 This provides information about HTTP2 related statistics in the Netscaler product.

http2Requests

OID: 1.3.6.1.4.1.5951.4.1.1.90.1 Total number of http2 requests

http2Responses

OID: 1.3.6.1.4.1.5951.4.1.1.90.2 Total number of http2 responses

http2Direct

OID: 1.3.6.1.4.1.5951.4.1.1.90.3 Total number of http2 direct connections established

http2ReqUpg

OID: 1.3.6.1.4.1.5951.4.1.1.90.4 Total number of connections upgraded to HTTP2

http2TotGrpcRequest

OID: 1.3.6.1.4.1.5951.4.1.1.90.5 Total number of gRPC requests

http2TotGrpcResponse

OID: 1.3.6.1.4.1.5951.4.1.1.90.6 Total number of gRPC responses

http2TotGrpcSuccess

OID: 1.3.6.1.4.1.5951.4.1.1.90.7 Total number of gRPC success

http2TotGrpcFailure

OID: 1.3.6.1.4.1.5951.4.1.1.90.8 Total number of gRPC failures

http2NoMatCipher

OID: 1.3.6.1.4.1.5951.4.1.1.90.9 Total number of cipher mismatch failures

http2PingFlood

OID: 1.3.6.1.4.1.5951.4.1.1.90.10 HTTP/2 number of ping frames received on connection is above rate limit

http2ErrSetFlood

OID: 1.3.6.1.4.1.5951.4.1.1.90.11 HTTP/2 number of settings frames received on connection is above rate limit

http2ErrResFraFlood

OID: 1.3.6.1.4.1.5951.4.1.1.90.12 HTTP/2 number of reset frames sent on connection is above rate limit

http2ErrEmpFraFlood

OID: 1.3.6.1.4.1.5951.4.1.1.90.13 HTTP/2 number of empty frames received on connection is above rate limit

http2DataFramesRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.90.14 Number of HTTP/2 DATA frames received

http2HeaderFramesRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.90.15 Total number of http2 header frames received

http2PriorityFramesRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.90.16 Total number of http2 priority frames received

http2RstStreamFramesRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.90.17 Number of HTTP/2 RST_STREAM frames received

http2SettingFramesRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.90.18 Number of HTTP/2 SETTINGS frames received

http2PushPromFramesRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.90.19 Number of HTTP/2 PUSH_PROMISE frames received

http2PingFramesRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.90.20 Number of HTTP/2 PING frames received

http2GoAwayFramesRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.90.21 Number of HTTP/2 GOAWAY frames received

http2WinUpdateFramesRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.90.22 Number of HTTP/2 WINDOW_UPDATE frames received

http2ContinuationFramesRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.90.23 Number of HTTP/2 CONTINUATION frames received

http2DataFramesSent

OID: 1.3.6.1.4.1.5951.4.1.1.90.24 Number of HTTP/2 DATA frames sent

http2HeaderFramesSent

OID: 1.3.6.1.4.1.5951.4.1.1.90.25 Number of HTTP/2 HEADER frames sent

http2PriorityFramesSent

OID: 1.3.6.1.4.1.5951.4.1.1.90.26 Number of HTTP/2 PRIORITY frames sent

http2RstStreamFramesSent

OID: 1.3.6.1.4.1.5951.4.1.1.90.27 Number of HTTP/2 RST_STREAM frames sent

http2SettingFramesSent

OID: 1.3.6.1.4.1.5951.4.1.1.90.28 Number of HTTP/2 SETTINGS frames sent

http2PushPromiseFramesSent

OID: 1.3.6.1.4.1.5951.4.1.1.90.29 Number of HTTP/2 PUSH_PROMISE frames sent

http2PingFramesSent

OID: 1.3.6.1.4.1.5951.4.1.1.90.30 Number of HTTP/2 PING frames sent

http2GoAwayFramesSent

OID: 1.3.6.1.4.1.5951.4.1.1.90.31 Number of HTTP/2 GOAWAY frames sent

http2WindowUpdateFramesSent

OID: 1.3.6.1.4.1.5951.4.1.1.90.32 Number of HTTP/2 WINDOW_UPDATE frames sent

http2ContinuationFramesSent

OID: 1.3.6.1.4.1.5951.4.1.1.90.33 Number of HTTP/2 CONTINUATION frames sent

http2InDataFrames

OID: 1.3.6.1.4.1.5951.4.1.1.90.34 Number of HTTP/2 DATA frames

http2InHeaderFrames

OID: 1.3.6.1.4.1.5951.4.1.1.90.35 Number of HTTP/2 HEADER frames

http2InPriorityFrames

OID: 1.3.6.1.4.1.5951.4.1.1.90.36 Number of HTTP/2 PRIORITY frames

http2InRstStreamFrames

OID: 1.3.6.1.4.1.5951.4.1.1.90.37 Number of HTTP/2 RST_STREAM frames

http2InSettingFrames

OID: 1.3.6.1.4.1.5951.4.1.1.90.38 Number of HTTP/2 SETTINGS frames

http2InPushPromiseFrames

OID: 1.3.6.1.4.1.5951.4.1.1.90.39 Number of HTTP/2 PUSH_PROMISE frames

http2InPingFrames

OID: 1.3.6.1.4.1.5951.4.1.1.90.40 Number of HTTP/2 PING frames

http2InGoAwayFrames

OID: 1.3.6.1.4.1.5951.4.1.1.90.41 Number of HTTP/2 GOAWAY frames

http2InWindowUpdateFrames

OID: 1.3.6.1.4.1.5951.4.1.1.90.42 Number of HTTP/2 WINDOW_UPDATE frames

http2InContinuationFrames

OID: 1.3.6.1.4.1.5951.4.1.1.90.43 Number of HTTP/2 CONTINUATION frames

http2ServerUpgradeFailed

OID: 1.3.6.1.4.1.5951.4.1.1.90.44 Number of HTTP/2 server upgrade failed

http2ServerDirectFailed

OID: 1.3.6.1.4.1.5951.4.1.1.90.45 Number of HTTP/2 server direct failed

http2ServerDirect

OID: 1.3.6.1.4.1.5951.4.1.1.90.46 Number of HTTP/2 server direct

http2RequestUpgradeFailed

OID: 1.3.6.1.4.1.5951.4.1.1.90.47 Number of HTTP/2 request upgrade failed

http2FrameTooBig

OID: 1.3.6.1.4.1.5951.4.1.1.90.48 Number of HTTP/2 frames received carrying a frame length greater than SETTINGS_MAX_FRAME_SIZE sent by NetScale

http2AltSvcFramesSent

OID: 1.3.6.1.4.1.5951.4.1.1.90.49 Number of HTTP/2 ALTSVC frames sent

http2ErrRxResFraFlood

OID: 1.3.6.1.4.1.5951.4.1.1.90.50 HTTP/2 number of reset frames received on connection is above rate limit

icapStatistics

OID: 1.3.6.1.4.1.5951.4.1.1.91.1 This provides information about ICAP Inspection

icapReqmodRequests

OID: 1.3.6.1.4.1.5951.4.1.1.91.1.1 Number of requests sent to ICAP Server

icapRespmodRequests

OID: 1.3.6.1.4.1.5951.4.1.1.91.1.2 Number of responses sent for Intrusion DEtection

icapPreviewEnabledRequests

OID: 1.3.6.1.4.1.5951.4.1.1.91.1.3 Number of preview requests for ICAP

icap204EnabledRequests

OID: 1.3.6.1.4.1.5951.4.1.1.91.1.4 Number of 204 Rquests

icap100ContRecv

OID: 1.3.6.1.4.1.5951.4.1.1.91.1.5 Number of 100-continue responses received

icap204NoContentRecv

OID: 1.3.6.1.4.1.5951.4.1.1.91.1.6 Number of 204 No content responses received

icapAdaptiveRequests

OID: 1.3.6.1.4.1.5951.4.1.1.91.1.7 Number of Adaptive requests

icapAdaptiveResponses

OID: 1.3.6.1.4.1.5951.4.1.1.91.1.8 Number of Adaptive Responses

icapCalloutInitiated

OID: 1.3.6.1.4.1.5951.4.1.1.91.1.9 Number of callout Requests started

icapCalloutCompleted

OID: 1.3.6.1.4.1.5951.4.1.1.91.1.10 Number of callout requests finished

icapErrorsHandled

OID: 1.3.6.1.4.1.5951.4.1.1.91.1.11 Number of errors sent

icapServerdownReset

OID: 1.3.6.1.4.1.5951.4.1.1.91.1.12 Number of requests for which serverdown Reset Action is taken

icapServerdownDrop

OID: 1.3.6.1.4.1.5951.4.1.1.91.1.13 Number of requests for which serverdown Drop Action is taken

icapServerdownBypass

OID: 1.3.6.1.4.1.5951.4.1.1.91.1.14 Number of requests for which serverdown Bypass Action is taken

inlineStatistics

OID: 1.3.6.1.4.1.5951.4.1.1.91.2 This provides information about ICAP Inspection

inlineRequestsSent

OID: 1.3.6.1.4.1.5951.4.1.1.91.2.1 HTTP/HTTPS requests sent for ContentInspection.

inlineResponsesSent

OID: 1.3.6.1.4.1.5951.4.1.1.91.2.2 HTTP/HTTPS responses sent for ContentInspection.

inlineReqBytesSent

OID: 1.3.6.1.4.1.5951.4.1.1.91.2.3 Number of bytes transfered for requests to IPS

inlineReqBytesRecv

OID: 1.3.6.1.4.1.5951.4.1.1.91.2.4 Number of bytes received for requests from IPS

inlineRespBytesSent

OID: 1.3.6.1.4.1.5951.4.1.1.91.2.5 Number of bytes transfered for responses to IPS

inlineRespBytesRecv

OID: 1.3.6.1.4.1.5951.4.1.1.91.2.6 Number of bytes received for responses from IPS

inlineServerdownReset

OID: 1.3.6.1.4.1.5951.4.1.1.91.2.7 Number of requests Reset when Inline device is down

inlineServerdownDrop

OID: 1.3.6.1.4.1.5951.4.1.1.91.2.8 Number of requests Dropped when Inline device is down

inlineServerdownBypass

OID: 1.3.6.1.4.1.5951.4.1.1.91.2.9 Number of requests bypass content Inspection Module when Inline device is down

inlineGeneratedResponses

OID: 1.3.6.1.4.1.5951.4.1.1.91.2.10 Number of Inline device generated Responses

mirrorStatistics

OID: 1.3.6.1.4.1.5951.4.1.1.91.3 This provides information about ICAP Inspection

mirrorRequestsSent

OID: 1.3.6.1.4.1.5951.4.1.1.91.3.1 Number of requests sent for Intrusion Detection

mirrorResponsesSent

OID: 1.3.6.1.4.1.5951.4.1.1.91.3.2 Number of responses sent for Intrusion Detection

mirrorReqBytesSent

OID: 1.3.6.1.4.1.5951.4.1.1.91.3.3 Number of request Bytes sent for Intrusion Detection

mirrorRespBytesSent

OID: 1.3.6.1.4.1.5951.4.1.1.91.3.4 Number of response Bytes sent for Intrusion Detection

mirrorServerdownReset

OID: 1.3.6.1.4.1.5951.4.1.1.91.3.5 Number of requests Reset when Mirror device is down

mirrorServerdownDrop

OID: 1.3.6.1.4.1.5951.4.1.1.91.3.6 Number of requests Dropped when Mirror device is down

mirrorServerdownBypass

OID: 1.3.6.1.4.1.5951.4.1.1.91.3.7 Number of requests bypass ContentInspection module when Mirror device is down

nsQuicStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.92 This provides information about QUIC Statistics in Citrix ADC

quicMigratedConn

OID: 1.3.6.1.4.1.5951.4.1.1.92.1 Total number of migrated QUIC connections

quicJumboFramesRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.92.2 Total number of QUIC jumbo frames received

quicTotClientConn

OID: 1.3.6.1.4.1.5951.4.1.1.92.3 Total QUIC client connections

quicTotServerConn

OID: 1.3.6.1.4.1.5951.4.1.1.92.4 Total QUIC server connections

quicCurClientConn

OID: 1.3.6.1.4.1.5951.4.1.1.92.5 Current QUIC client connections

quicCurServerConn

OID: 1.3.6.1.4.1.5951.4.1.1.92.6 Current QUIC server connections

quicClientDgrmRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.92.7 Total QUIC client UDP datagrams received

quicServerDgrmRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.92.8 Total QUIC server UDP datagrams received

quicClientDgrmSent

OID: 1.3.6.1.4.1.5951.4.1.1.92.9 Total QUIC client UDP datagrams sent

quicServerDgrmSent

OID: 1.3.6.1.4.1.5951.4.1.1.92.10 Total QUIC server UDP datagrams sent

quicLocalConnID

OID: 1.3.6.1.4.1.5951.4.1.1.92.11 Current QUIC local connection IDs allocated

quicTLSAlertSent

OID: 1.3.6.1.4.1.5951.4.1.1.92.12 Total QUIC TLS 1.3 transport errors sent

quicRetryPktSent

OID: 1.3.6.1.4.1.5951.4.1.1.92.13 Number of QUIC Retry packets sent

quicStlessConnClosePktSent

OID: 1.3.6.1.4.1.5951.4.1.1.92.14 Number of QUIC stateless Connection Close packets sent

quicVerNegPktSent

OID: 1.3.6.1.4.1.5951.4.1.1.92.15 Number of QUIC Version Negotiation packets sent

quicHandshakeCmpltd

OID: 1.3.6.1.4.1.5951.4.1.1.92.16 Number of QUIC handshake messages completed

quicTransptConnClosePktSent

OID: 1.3.6.1.4.1.5951.4.1.1.92.17 Number of QUIC transport no-error Connection Close packets sent

quicTransptConnClosePktFail

OID: 1.3.6.1.4.1.5951.4.1.1.92.18 Number of QUIC transport error Connection Close packets sent

quicAppConnClosePktSent

OID: 1.3.6.1.4.1.5951.4.1.1.92.19 Number of QUIC application no-error Connection Close packets sent

quicAppConnClosePktFail

OID: 1.3.6.1.4.1.5951.4.1.1.92.20 Number of QUIC application error Connection Close packets sent

quicRetryTokenVerFail

OID: 1.3.6.1.4.1.5951.4.1.1.92.21 Number of times QUIC Retry token verification failed

quicNewTokenVerFail

OID: 1.3.6.1.4.1.5951.4.1.1.92.22 Number of times QUIC NEW_TOKEN token verification failed

quicCurSavedCryptoCtx

OID: 1.3.6.1.4.1.5951.4.1.1.92.23 Current QUIC crypto contexts allocated

quicAsyncDatagramsSent

OID: 1.3.6.1.4.1.5951.4.1.1.92.24 Number of QUIC datagrams sent using async mode

nsQuicBridgeStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.93 This provides information about QUIC BRIDGE Statistics in Citrix ADC

quicBridgeConn

OID: 1.3.6.1.4.1.5951.4.1.1.93.1 Total number of QUIC Bridge connections

quicBridgeMigratedConn

OID: 1.3.6.1.4.1.5951.4.1.1.93.2 Total number of migrated QUIC Bridge connections

quicBridgeQci

OID: 1.3.6.1.4.1.5951.4.1.1.93.3 Current number of QUIC Bridge connection infos

quicBridgeQpi

OID: 1.3.6.1.4.1.5951.4.1.1.93.4 Current number of QUIC Bridge peer infos

nsHttp3StatsGroup

OID: 1.3.6.1.4.1.5951.4.1.1.94 This provides information about HTTP3 Statistics in Citrix ADC

http3RequestsRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.94.1 Total number of HTTP/3 requests received

http3ResponsesSent

OID: 1.3.6.1.4.1.5951.4.1.1.94.2 Total number of HTTP/3 responses sent

http3RequestsSent

OID: 1.3.6.1.4.1.5951.4.1.1.94.3 Total number of HTTP/3 requests sent

http3ResponsesRcvd

OID: 1.3.6.1.4.1.5951.4.1.1.94.4 Total number of HTTP/3 responses received

apiSpecTable

OID: 1.3.6.1.4.1.5951.4.1.1.95.1

This is indexed on the apiSpecName .

apiSpecName

OID: 1.3.6.1.4.1.5951.4.1.1.95.1.1.1 API specification name

apiSpecFullName

OID: 1.3.6.1.4.1.5951.4.1.1.95.1.1.2 API specification full name

apispecHits

OID: 1.3.6.1.4.1.5951.4.1.1.95.1.1.3 Number of received requests for the API specification.

apispecSuccessfullyValidated

OID: 1.3.6.1.4.1.5951.4.1.1.95.1.1.4 Number of successfully validated requests for the API specification.

apispecUnmatched

OID: 1.3.6.1.4.1.5951.4.1.1.95.1.1.5 Number of requests non matching this API specification.

apiEndpointTable

OID: 1.3.6.1.4.1.5951.4.1.1.95.2

This is indexed on the apiEpName .

apiEpName

OID: 1.3.6.1.4.1.5951.4.1.1.95.2.1.1 API endpoint name

apiEpFullName

OID: 1.3.6.1.4.1.5951.4.1.1.95.2.1.2 API endpoint full name

apiEndpointHits

OID: 1.3.6.1.4.1.5951.4.1.1.95.2.1.3 Number of received requests for the API endpoint.

apiEndpointSuccessfullyValidated

OID: 1.3.6.1.4.1.5951.4.1.1.95.2.1.4 Number of successfully validated requests for the API endpoint.

serviceTable

OID: 1.3.6.1.4.1.5951.4.1.2.1 The netscaler services table This is indexed on the svcServiceName.

svcServiceName

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.1 The name of the service.

svcIpAddress

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.2 The ip address at which the service is running.

svcPort

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.3 The port at which the service is running.

svcServiceType

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.4 The protocol type of the service

svcState

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.5

Current

OID:state

svcMaxReqPerConn

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.6 Maximum requests per connection allowed on this service.

svcAvgTransactionTime

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.7 Average transaction time in microseconds between Citrix ADC and the service behind it.

svcEstablishedConn

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.8 Total number of connections in ESTABLISHED state.

svcActiveConn

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.9 Number of connections that are currently active.

svcSurgeCount

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.10 Number of requests in the surge queue.

svcTotalRequests

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.30

Total

OID:number

svcTotalRequestBytes

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.31 Total number of request bytes received on this service or virtual server.

svcTotalResponses

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.32

Number

OID:of

svcTotalResponseBytes

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.33 Number of response bytes received by this service or virtual server.

svcTotalPktsRecvd

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.34 Total number of packets received by this service or virtual server.

svcTotalPktsSent

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.35 Total number of packets sent.

svcTotalSynsRecvd

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.36 Total number of SYN packets received from clients on this service (only when directly accessed) or virtual server.

svcGslbSiteName

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.37 The name of the gslb site on which this service is defined.

svcAvgSvrTTFB

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.38 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

svctotalJsTransactions

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.39 Total number of javascripts sent to geniune clients.

svcdosQDepth

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.40 Number of clients waiting currently in priority queue

svcCurClntConnections

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.41 Number of current client connections.

svcRequestRate

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.42 Request rate in requests per second for this service or virtual server.

svcRxBytesRate

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.43 Request rate in bytes per second fot this service or virtual server.

svcTxBytesRate

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.44 Response rate in bytes per second for this service or virtual server.

svcSynfloodRate

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.45 Rate of unacknowledged SYN packets for this service or virtual server.

svcTicksSinceLastStateChange

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.47 Time (in 10 milliseconds) since the last state change.

svcTotalClients

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.48 Total number of established client connections.

svcTotalServers

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.49 Total number of established server connections.

svcMaxClients

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.52 Maximum open connections allowed on this service.

svcActiveTransactions

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.53 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

svcServiceFullName

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.54 The name of the service.

svcInetAddressType

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.55 The address type of svcInetAddress

svcInetAddress

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.56 The Internet address at which the service is running.

svcTdId

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.57 Traffic Domain ID of this service.

svcGslbState

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.58

Effective

OID:state

svcCurSrvrConnections

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.59 Number of current connections to the actual servers behind the virtual server.

svctotalConnReassemblyQueueFlush

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.60 Total no of connections incurred TCP reassembly queue flush

svctotalConnReassemblyQueue75

OID: 1.3.6.1.4.1.5951.4.1.2.1.1.61 Total no of connections with 75% TCP reassembly queue

serverTable

OID: 1.3.6.1.4.1.5951.4.1.2.2 The servers table. This is indexed on the serverName .

serverName

OID: 1.3.6.1.4.1.5951.4.1.2.2.1.1 The name of the server.

serverIpAddress

OID: 1.3.6.1.4.1.5951.4.1.2.2.1.2 The IP address of the server.

serverState

OID: 1.3.6.1.4.1.5951.4.1.2.2.1.3 The state of the server.

serverDelay

OID: 1.3.6.1.4.1.5951.4.1.2.2.1.4 Specifies time in seconds after which all services in this server are brought down.

serverFullName

OID: 1.3.6.1.4.1.5951.4.1.2.2.1.5 The name of the server.

serverInetAddressType

OID: 1.3.6.1.4.1.5951.4.1.2.2.1.6 The address type of serverInetAddress

serverInetAddress

OID: 1.3.6.1.4.1.5951.4.1.2.2.1.7 The Internet address of the server.

serverTdId

OID: 1.3.6.1.4.1.5951.4.1.2.2.1.8 Traffic Domain ID of this server.

serviceScpolicyTable

OID: 1.3.6.1.4.1.5951.4.1.2.3 The service sure connect policy relationship table This is indexed on the svcServiceName and scPolicyName](#)](#)](#) .

svcscpolicyPrimaryIPAddress

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.3 The IP address of the service or virtual server to which the policy is bound.

svcscpolicyPrimaryPort

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.4 The port of the service or virtual server to which the policy is bound.

svcscpolicydesIpAddress

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.10 IP address of the destination service.

svcscpolicydestPort

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.11 Port number of the destination service.

svcscpolicyavgServerTransactionTime

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.12 Average server transaction time in seconds for this SureConnect Policy.

svcscpolicytotClientTransaction

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.13 Total number of client transactions processed by this SureConnect policy.

svcscpolicytotOpenConn

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.14 Current number of open connections to the servers matching this policy.

svcscpolicyscPhysicalServiceIP

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.15 IP address of the service for which these statistics are maintained.

svcscpolicyscPhysicalServicePort

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.16 Port of the service for which these statistics are maintained.

svcscpolicyscCurrentWaitingTime

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.17 Value of the currently estimated waiting time in seconds for the configured URL.

svcscpolicyscCurrentClientConnections

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.18 Number of clients currently allowed a server connection by this SureConnect policy.

svcscpolicyscTotalClientConnections

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.19 Total number of clients that were allowed a server connection by this SureConnect policy.

svcscpolicyscTotalServerConnections

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.20 Total number of server connections that were established through this SureConnect policy.

svcscpolicyscTotalRequestsReceived

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.21 Total number of requests received by this SureConnect policy.

svcscpolicyscTotalRequestBytes

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.22 Total number of request bytes received by this SureConnect policy.

svcscpolicyscTotalResponsesReceived

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.23 Total number of server responses received by this SureConnect policy.

svcscpolicyscTotalResponseBytes

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.24 Total number of response bytes received by this SureConnect policy.

svcscpolicyscCurrentSurgeQClients

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.25 Number of clients currently matching the SureConnect policy, but are in the surge queue.

svcscpolicyscCurrentWaitingClients

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.26 Current number of SureConnect priority clients that are waiting for a server connection.

svcscpolicyscTotalServerTransactions

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.27 Number of 200 OK responses received from the web server by this SureConnect policy.

svcscpolicyscTotalServerTTFBTransactions

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.28 Number of Time-To-First-Byte transcations from the web server for this SureConnect policy.

svcscpolicyscTotalServerTTLB

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.29 Server Time-To-Last-Byte in seconds calculated for this SureConnect policy.

svcscpolicyscTotalClientTTLB

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.30 Client Time-To-Last-Byte in seconds calculated for this SureConnect policy.

svcscpolicyscTotalServerTTFB

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.31 Server Time-To-First-Byte in seconds calculated for this SureConnect policy.

svcscpolicyscAverageClientTTLB

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.32 Average value of the client Time-To-Last-Byte in seconds for this SureConnect policy.

svcscpolicyscAverageServerTTFB

OID: 1.3.6.1.4.1.5951.4.1.2.3.1.33 Average value of the server Time-To-First-Byte in seconds for this SureConnect policy.

serviceAdvanceSslConfigTable

OID: 1.3.6.1.4.1.5951.4.1.2.4 The service advance SSL configuration This is indexed on the svcServiceName.

svcSslDH

OID: 1.3.6.1.4.1.5951.4.1.2.4.1.1 Whether DH is enabled/disabled.

svcSslDHCount

OID: 1.3.6.1.4.1.5951.4.1.2.4.1.2 The DH refresh count to re-generate public/private key.

svcSslDHFilePath

OID: 1.3.6.1.4.1.5951.4.1.2.4.1.3 The DH file path name.

svcSsleRSA

OID: 1.3.6.1.4.1.5951.4.1.2.4.1.4 The ephimeral RSA support for service.

svcSsleRSACount

OID: 1.3.6.1.4.1.5951.4.1.2.4.1.5 The eRSA refresh count to re-generate RSA temporary key.

svcSslv2Protocol

OID: 1.3.6.1.4.1.5951.4.1.2.4.1.6 The support for SSLv2 protocol for service.

svcSslv3Protocol

OID: 1.3.6.1.4.1.5951.4.1.2.4.1.7 The support for SSLv3 protocol for service.

svcSslTLSv1Protocol

OID: 1.3.6.1.4.1.5951.4.1.2.4.1.8 The support for TLSv1 protocol for service.

svcSslRedirectSupport

OID: 1.3.6.1.4.1.5951.4.1.2.4.1.9 The support for ssl redirect for service.

svcSslClearTextPort

OID: 1.3.6.1.4.1.5951.4.1.2.4.1.10 The clear text port on the backend webserver.

serviceCipherBindingTable

OID: 1.3.6.1.4.1.5951.4.1.2.5 The service cipher bindings This is indexed on the svcServiceName and svcSslCipherBindName](#)](#) See "Citrix ADC Enterprise OIDs" on page 37 .

svcSslCipherBindName

OID: 1.3.6.1.4.1.5951.4.1.2.5.1.1 The cipher name bound to this service.

svcSslCipherBindDesc

OID: 1.3.6.1.4.1.5951.4.1.2.5.1.2 The Cipher description.

serviceGlobalStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.2.6 This provides information about service related statictics in the Netscaler product.

svcCount

OID: 1.3.6.1.4.1.5951.4.1.2.6.1 Number of services defined on this Citrix ADC.

serverCount

OID: 1.3.6.1.4.1.5951.4.1.2.6.2 Number of servers defined on this Citrix ADC.

svcgroupCount

OID: 1.3.6.1.4.1.5951.4.1.2.6.3 Number of service groups defined on this Citrix ADC.

svcgroupmemCount

OID: 1.3.6.1.4.1.5951.4.1.2.6.4 Number of service group members defined on this Citrix ADC.

syssvcCount

OID: 1.3.6.1.4.1.5951.4.1.2.6.5 Number of services configured on this Citrix ADC.

sysupsvcCount

OID: 1.3.6.1.4.1.5951.4.1.2.6.6 Number of configured services which are up on this Citrix ADC.

sysupsvcitmCount

OID: 1.3.6.1.4.1.5951.4.1.2.6.7 Number of configured service items which are up on this Citrix ADC.

serviceGroupMemberTable

OID: 1.3.6.1.4.1.5951.4.1.2.7 The service group member bindings This is indexed on the svcGrpMemberGroupName and svcGrpMemberName](#)](#)](#) .

svcGrpMemberGroupName

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.1 The name of the service Group

svcGrpMemberName

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.2 The name of the service group member

svcGrpMemberPrimaryIPAddress

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.3 The IP address on which the service is running.

svcGrpMemberPrimaryPort

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.4 The port on which the service is running.

svcGrpMemberServiceType

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.5 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

svcGrpMemberState

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.6

Current

OID:state

svcGrpMemberWeight

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.7 The weight of the service group member tied to the vserver.

svcGrpMemberMaxReqPerConn

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.8 Maximum requests per connection allowed on this service.

svcGrpMemberAvgTransactionTime

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.9 Average transaction time in microseconds between Citrix ADC and the service behind it.

svcGrpMemberEstablishedConn

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.10 Total number of connections in ESTABLISHED state.

svcGrpMemberActiveConn

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.11 Number of connections that are currently active.

svcGrpMemberSurgeCount

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.12 Number of requests in the surge queue.

svcGrpMemberTotalRequests

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.13

Total

OID:number

svcGrpMemberTotalRequestBytes

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.14 Total number of request bytes received on this service or virtual server.

svcGrpMemberTotalResponses

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.15

Number

OID:of

svcGrpMemberTotalResponseBytes

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.16 Number of response bytes received by this service or virtual server.

svcGrpMemberTotalPktsRecvd

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.17 Total number of packets received by this service or virtual server.

svcGrpMemberTotalPktsSent

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.18 Total number of packets sent.

svcGrpMemberTotalSynsRecvd

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.19 Total number of SYN packets received from clients on this service (only when directly accessed) or virtual server.

svcGrpMemberGslbSiteName

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.20 The name of the gslb site on which this service is defined.

svcGrpMemberAvgSvrTTFB

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.21 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

svcGrpMembertotalJsTransactions

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.22 Total number of javascripts sent to geniune clients.

svcGrpMemberdosQDepth

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.23 Number of clients waiting currently in priority queue

svcGrpMemberCurClntConnections

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.24 Number of current client connections.

svcGrpMemberRequestRate

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.25 Request rate in requests per second for this service or virtual server.

svcGrpMemberRxBytesRate

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.26 Request rate in bytes per second fot this service or virtual server.

svcGrpMemberTxBytesRate

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.27 Response rate in bytes per second for this service or virtual server.

svcGrpMemberSynfloodRate

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.28 Rate of unacknowledged SYN packets for this service or virtual server.

svcGrpMemberTicksSinceLastStateChange

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.31 Time (in 10 milliseconds) since the last state change.

svcGrpMemberGroupFullName

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.32 The name of the service Group

svcGrpMemberFullName

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.33 The name of the service group member

svcGrpMemberPrimaryInetAddressType

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.34 The address type of svcGrpMemberPrimaryInetAddress

svcGrpMemberPrimaryInetAddress

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.35 The Internet address at which the service is running.

svcGrpMemberServerName

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.36 The name of the server of the servicegroup member

svcGrpMemberTdId

OID: 1.3.6.1.4.1.5951.4.1.2.7.1.37 Traffic Domain ID of this service group member.

serviceDospolicyTable

OID: 1.3.6.1.4.1.5951.4.1.2.8 The service DOS policy relationship table This is indexed on the svcServiceName and dosPolicyName](#)](#)](#) .

svcdospolicydosTotJSSent

OID: 1.3.6.1.4.1.5951.4.1.2.8.1.1 Total number of DoS JavaScript transactions performed for this policy.

svcdospolicydosTotJSBytesSent

OID: 1.3.6.1.4.1.5951.4.1.2.8.1.2 Total number of DoS JavaScript bytes sent for this policy.

svcdospolicydosTotJSRefused

OID: 1.3.6.1.4.1.5951.4.1.2.8.1.3 Number of times the DoS JavaScript was not sent because the set JavaScript rate was not met for this policy.

svcdospolicydosTotNonGetPostRequests

OID: 1.3.6.1.4.1.5951.4.1.2.8.1.4 Number of non-GET and non-POST requests for which DOS JavaScript was sent.

svcdospolicydosPhysicalServiceIP

OID: 1.3.6.1.4.1.5951.4.1.2.8.1.5 IP address of the service to which this policy is bound.

svcdospolicydosPhysicalServicePort

OID: 1.3.6.1.4.1.5951.4.1.2.8.1.6 Port address of the service to which this policy is bound.

svcdospolicydosCurrentQueueSize

OID: 1.3.6.1.4.1.5951.4.1.2.8.1.7 Current queue size of the server to which this policy is bound.

svcdospolicydosCurrentJSRate

OID: 1.3.6.1.4.1.5951.4.1.2.8.1.8 Current rate at which JavaScript is being sent in response to client requests.

svcdospolicydosTotValidClients

OID: 1.3.6.1.4.1.5951.4.1.2.8.1.9 Total number of valid DoS cookies received for this policy.

svcdospolicydosCurServerRespRate

OID: 1.3.6.1.4.1.5951.4.1.2.8.1.10 Current rate at which the server to which this policy is bound is responding.

monitorMemberTable

OID: 1.3.6.1.4.1.5951.4.1.2.9 The monitor table This is indexed on the monitorName .

monitorName

OID: 1.3.6.1.4.1.5951.4.1.2.9.1.1 Monitor name

responseTimeoutThreshold

OID: 1.3.6.1.4.1.5951.4.1.2.9.1.2 Monitor Response timeout threshold, above which snmp trap will be fired.It is expressed in milliseconds.

monitorType

OID: 1.3.6.1.4.1.5951.4.1.2.9.1.3 Type of the monitor.

monitorInterval

OID: 1.3.6.1.4.1.5951.4.1.2.9.1.4 Interval between monitoring probes.It is expressed in milliseconds.

monitorResponseTimeout

OID: 1.3.6.1.4.1.5951.4.1.2.9.1.5 Maximum time a monitor probe can take to respond.It is expressed in milliseconds.

monitorDowntime

OID: 1.3.6.1.4.1.5951.4.1.2.9.1.6 Time for which the monitor probes are not fired once it is down.It is expressed in milliseconds.

monitorRetrys

OID: 1.3.6.1.4.1.5951.4.1.2.9.1.7 Number of failed attempts to make server DOWN.

destinationIP

OID: 1.3.6.1.4.1.5951.4.1.2.9.1.8 Destination IP address that is used for monitoring.

destinationPort

OID: 1.3.6.1.4.1.5951.4.1.2.9.1.9 Destination port that is used for monitoring.

drtmDeviation

OID: 1.3.6.1.4.1.5951.4.1.2.9.1.10 Tolerable Deviation of response time for DRTM.It is expressed in milliseconds.

drtmActiveMonitors

OID: 1.3.6.1.4.1.5951.4.1.2.9.1.11 Number of monitors contributing to DRTM average.

drtmCumResponseTimeout

OID: 1.3.6.1.4.1.5951.4.1.2.9.1.12 Total cumulative response time of all active DRTM monitors.It is expressed in milliseconds.

alarmProbeFailedRetries

OID: 1.3.6.1.4.1.5951.4.1.2.9.1.13 Number of failed attempts to generate snmp trap.

destinationInetAddressType

OID: 1.3.6.1.4.1.5951.4.1.2.9.1.14 The address type of destinationInetAddress

destinationInetAddress

OID: 1.3.6.1.4.1.5951.4.1.2.9.1.15 Destination Internet address that is used for monitoring.

monitorFullName

OID: 1.3.6.1.4.1.5951.4.1.2.9.1.16 Monitor Full name

monServiceMemberTable

OID: 1.3.6.1.4.1.5951.4.1.2.10 The moninfo table, bindings of monitors to services. This is indexed on the monServiceName and monitorName](#)](#)](#) .

monServiceName

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.1 The name of the service to which the monitor is bound.

monitorRTO

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.2

Response

OID:time

monitorState

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.3 State of the specified monitor. Possible states are UP, OUT OF SERVICE, DOWN, GOING OUT OF SERVICE, and DOWN WHEN GOING OUT OF SERVICE.

drtmRTO

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.4

Monitor

OID:probe

drtmLearningProbes

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.5 Current number of pending DRTM monitoring probes.

monitorCurFailedCount

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.6

Current

OID:continuous

monitorWeight

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.7 Weight assigned to the monitor binding.

alarmMonrespto

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.8 This is the response time taken for the current monitor probe.

monitorProbes

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.9 Number of monitoring probes sent.

monitorFailed

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.10 Number of failed monitoring probes.

monitorMaxClient

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.11 Number of monitoring probes that were not sent due to MaxClients.

monitorFailedCon

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.12 Number of failed monitoring probes due to failed connections.

monitorFailedCode

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.13 Number of failed monitoring probes due to improper response code.

monitorFailedStr

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.14 Number of failed monitoring probes due to invalid response string.

monitorFailedTimeout

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.15 Number of failed monitoring probes due to timeout.

monitorFailedSend

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.16 Number of failed monitoring probes due to inability to send the data.

monitorFailedFTP

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.17 Number of failed monitoring probes due to ftp protocol violation.

monitorFailedPort

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.18 Number of failed monitoring probes due to port unreachable response.

monitorFailedResponse

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.19 Number of failed monitoring probes due to invalid response.

monitorFailedId

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.20 Number of failed monitoring probes due to response id mismatch.

monitorProbesNoChange

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.21 Number of monitoring probes which did not change the state.

monitorResponseTimeoutThreshExceed

OID: 1.3.6.1.4.1.5951.4.1.2.10.1.22 Number of times the response time has exceeded the configured threshold.

serviceGroupTable

OID: 1.3.6.1.4.1.5951.4.1.2.11 The netscaler services group table This is indexed on the svcgrpSvcGroupName.

svcgrpSvcGroupName

OID: 1.3.6.1.4.1.5951.4.1.2.11.1.1 The name of the service Group

svcgrpSvcGroupType

OID: 1.3.6.1.4.1.5951.4.1.2.11.1.2 The type of the service Group.

svcgrpSvcGroupState

OID: 1.3.6.1.4.1.5951.4.1.2.11.1.3 The state of the service Group

svcgrpSvcGroupFullName

OID: 1.3.6.1.4.1.5951.4.1.2.11.1.4 The full name of the service Group

svcgrpTdId

OID: 1.3.6.1.4.1.5951.4.1.2.11.1.5 Traffic Domain ID of this service group.

vserverTable

OID: 1.3.6.1.4.1.5951.4.1.3.1 The vservers table This is indexed on the vsvrName.

vsvrName

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.1 The name of the vserver

vsvrIpAddress

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.2 IP address of the vserver

vsvrPort

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.3 the port of the vserver

vsvrType

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.4 Protocol associated with the vserver

vsvrState

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.5

Current

OID:state

vsvrCurClntConnections

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.7 Number of current client connections.

vsvrCurSrvrConnections

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.8 Number of current connections to the actual servers behind the virtual server.

vsvrSurgeCount

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.10 Number of requests in the surge queue.

vsvrTotalRequests

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.30

Total

OID:number

vsvrTotalRequestBytes

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.31 Total number of request bytes received on this service or virtual server.

vsvrTotalResponses

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.32

Number

OID:of

vsvrTotalResponseBytes

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.33 Number of response bytes received by this service or virtual server.

vsvrTotalPktsRecvd

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.34 Total number of packets received by this service or virtual server.

vsvrTotalPktsSent

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.35 Total number of packets sent.

vsvrTotalSynsRecvd

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.36 Total number of SYN packets received from clients on this service (only when directly accessed) or virtual server.

vsvrCurServicesDown

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.37 The current number of services which are bound to this vserver and are in the state 'down'.

vsvrCurServicesUnKnown

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.38 The current number of services which are bound to this vserver and are in the state 'unKnown'.

vsvrCurServicesOutOfSvc

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.39 The current number of services which are bound to this vserver and are in the state 'outOfService'.

vsvrCurServicesTransToOutOfSvc

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.40 The current number of services which are bound to this vserver and are in the state 'transitionToOutOfService'.

vsvrCurServicesUp

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.41 The current number of services which are bound to this vserver and are in the state 'up'.

vsvrTotMiss

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.42 Total vserver misses

vsvrRequestRate

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.43 Request rate in requests per second for this service or virtual server.

vsvrRxBytesRate

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.44 Request rate in bytes per second fot this service or virtual server.

vsvrTxBytesRate

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.45 Response rate in bytes per second for this service or virtual server.

vsvrSynfloodRate

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.46 Rate of unacknowledged SYN packets for this service or virtual server.

vsvrIp6Address

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.47 IPv6 address of the v server

vsvrTotHits

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.48 Total vserver hits

vsvrTotSpillOvers

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.54 Number of times vserver experienced spill over.

vsvrTotalClients

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.56 Total number of established client connections.

vsvrClientConnOpenRate

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.58 Rate at which connections are opened for this virtual server per second.

vsvrFullName

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.59 The name of the vserver

vsvrCurSslVpnUsers

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.60 Number of aaa sessions on this vserver

vsvrTotalServicesBound

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.61 The current number of services which are bound to this vserver.

vsvrHealth

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.62 The percentage of UP services bound to this vserver.

vsvrTicksSinceLastStateChange

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.63 Time (in 10 milliseconds) since the last state change.

vsvrEntityType

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.64 The type of the vserver.

vsvrTotalServers

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.65 Total number of established server connections.

vsvrActiveActiveState

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.66 The state of the vserver based on ActiveActive configuration.

vsvrInvalidRequestResponse

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.67 Number invalid requests/responses on this vserver

vsvrInvalidRequestResponseDropped

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.68 Number invalid requests/responses dropped on this vserver

vsvrTdId

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.69 Traffic Domain of the vserver

vsvrSoThreshold

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.70 Spill Over Threshold set on the VServer.

vsvrEstablishedConn

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.71 Number of client connections in ESTABLISHED state.

vsvrCurTotalVpnUsers

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.72 Number of users on this vserver

vsvrCurMptcpSessions

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.73 Current Multipath TCP sessions

vsvrCursubflowConn

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.74 Current Multipath TCP subflows

vsvrCurEffState

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.75 Current Effective state of vserver

vsvrCurPersistenceSessions

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.76 current vserver owned persistence sessions

vsvrCurBackupPersistenceSessions

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.77 current vserver owned backup persistence sessions

vsvrtotalConnReassemblyQueueFlush

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.78 Total no of connections incurred TCP reassembly queue flush

vsvrtotalConnReassemblyQueue75

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.79 Total no of connections with 75% TCP reassembly queue

vsvrtotalSvrBusyErr

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.80 Total no of server busy error

vsvrBackupVserver

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.81 Name of the backup Vserver

vsvrTotalH2Responses

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.82

Number

OID:of

vsvrTotalH2Requests

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.83

Total

OID:number

vsvrCpuUsagePm

OID: 1.3.6.1.4.1.5951.4.1.3.1.1.84 Vserver CPU usage in per-mille(parts per thousand)

vserverServiceTable

OID: 1.3.6.1.4.1.5951.4.1.3.2 The vserver service relationship table This is indexed on the vsvrName and vsvrServiceName](#)](#)](#) .

vsvrServiceHits

OID: 1.3.6.1.4.1.5951.4.1.3.2.1.5 Number of times that the service has been provided.

servicePersistentHits

OID: 1.3.6.1.4.1.5951.4.1.3.2.1.6 Total number of persistent hits.

serviceWeight

OID: 1.3.6.1.4.1.5951.4.1.3.2.1.7 The weight of the service tied to the vserver.

vsvrServiceName

OID: 1.3.6.1.4.1.5951.4.1.3.2.1.8 The name of the service to which the vserver is bound.

vsvrServiceFullName

OID: 1.3.6.1.4.1.5951.4.1.3.2.1.9 The Full name of the service to which the vserver is bound.

vserverFullName

OID: 1.3.6.1.4.1.5951.4.1.3.2.1.10 The full name of the vserver.

vsvrServiceEntityType

OID: 1.3.6.1.4.1.5951.4.1.3.2.1.11 The entity type of the service: service group member or service.

vserverCspolicyTable

OID: 1.3.6.1.4.1.5951.4.1.3.3 The vserver content switching policy relationship table for PE CS Policy This is indexed on the vsvrName and cspolicyName](#)](#)](#) .

cspolicyName

OID: 1.3.6.1.4.1.5951.4.1.3.3.1.1 This represents the name of the CS PE policy bound to content switching vserver

cspolicyDestVserverName

OID: 1.3.6.1.4.1.5951.4.1.3.3.1.2 This represents the name of the destination vserver to which the request has to be directed to if the content switching policy evaluates to true.

cspolicyHits

OID: 1.3.6.1.4.1.5951.4.1.3.3.1.5 The number of hits on this content switching policy.

csIndexVserverFullName

OID: 1.3.6.1.4.1.5951.4.1.3.3.1.6 The full name of the cs vserver to which this policy belongs.

vserverCrpolicyTable

OID: 1.3.6.1.4.1.5951.4.1.3.4 The vserver cache redirection policy relationship table This is indexed on the vsvrName and crpolicyName](#)](#)](#) .

crpolicyName

OID: 1.3.6.1.4.1.5951.4.1.3.4.1.1 This represents the name of the policy bound to cache-redirection vserver

crpolicyHits

OID: 1.3.6.1.4.1.5951.4.1.3.4.1.4 Hits on the cache redirection policy.

crIndexVserverFullName

OID: 1.3.6.1.4.1.5951.4.1.3.4.1.5 The full name of the cr vserver to which this policy belongs.

vserverGlobalStatsGroup

OID: 1.3.6.1.4.1.5951.4.1.3.5 This provides information about vserver related statictics in the Netscaler product.

curConfigVservers

OID: 1.3.6.1.4.1.5951.4.1.3.5.1 Total number of vservers configured on the Citrix ADC.

vsvrBindCount

OID: 1.3.6.1.4.1.5951.4.1.3.5.2 Number of virtual server bindings on this Citrix ADC.

vsvrSvcGrpBindCount

OID: 1.3.6.1.4.1.5951.4.1.3.5.3 Number of virtual server, service group bindings on this Citrix ADC.

curConfigLbVservers

OID: 1.3.6.1.4.1.5951.4.1.3.5.4 Total number of LB vservers configured on the Citrix ADC.

curConfigGslbVservers

OID: 1.3.6.1.4.1.5951.4.1.3.5.5 Total number of GSLB vservers configured on the Citrix ADC.

totSpilloverCount

OID: 1.3.6.1.4.1.5951.4.1.3.5.6 Total count of spillovers.

lbvserverTable

OID: 1.3.6.1.4.1.5951.4.1.3.6 Table for LB specific configuration This is indexed on the vsvrName.

lbvsvrLBMethod

OID: 1.3.6.1.4.1.5951.4.1.3.6.1.1 The Policy used for Load Balancing.

lbvsvrPersistanceType

OID: 1.3.6.1.4.1.5951.4.1.3.6.1.2 The type of persistence used.

lbvsvrPersistenceTimeOut

OID: 1.3.6.1.4.1.5951.4.1.3.6.1.3 The timeout set for persistence.

lbvsvrActiveConn

OID: 1.3.6.1.4.1.5951.4.1.3.6.1.4 Number of connections that are currently active.

lbvsvrAvgSvrTTFB

OID: 1.3.6.1.4.1.5951.4.1.3.6.1.5 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

lbvsvrRdpCookieParsed

OID: 1.3.6.1.4.1.5951.4.1.3.6.1.6 Number of times MSTS RDP Cookie got parsed on this vserver

vserverPqpolicyTable

OID: 1.3.6.1.4.1.5951.4.1.3.7 The vserver priority queuing policy relationship table This is indexed on the vsvrName and pqName](#)](#)](#) .

pqpolicytotClientTransactionTime

OID: 1.3.6.1.4.1.5951.4.1.3.7.1.5 Total client transaction time in micro-seconds for this priority queuing policy.

pqpolicytotClientTransactions

OID: 1.3.6.1.4.1.5951.4.1.3.7.1.6 Total number of client transactions for this priority queuing policy.

pqpolicypqDropped

OID: 1.3.6.1.4.1.5951.4.1.3.7.1.7 Total number of dropped transactions for this priority queuing policy.

pqpolicypqQdepth

OID: 1.3.6.1.4.1.5951.4.1.3.7.1.8 Number of clients waiting currently for this priority queuing policy.

pqpolicypqAvgClientTransactionTime

OID: 1.3.6.1.4.1.5951.4.1.3.7.1.9 Average time taken by a priority queuing client to complete its transaction for this priority queuing policy.

pqpolicypqVserverIP

OID: 1.3.6.1.4.1.5951.4.1.3.7.1.10 IP address of the virtual server to which this priority queuing policy is bound.

pqpolicypqVserverPort

OID: 1.3.6.1.4.1.5951.4.1.3.7.1.11 Port number of the virtual server to which this priority queuing policy is bound.

pqpolicypqCurrentClientConnections

OID: 1.3.6.1.4.1.5951.4.1.3.7.1.12 Current number of server connections established for serving clients for this priority queuing policy.

pqpolicypqTotQueueDepth

OID: 1.3.6.1.4.1.5951.4.1.3.7.1.13 Total number of waiting clients for this priority queuing policy.

pqpolicypqTotClientConnections

OID: 1.3.6.1.4.1.5951.4.1.3.7.1.14 Total number of server connections established for serving clients for this priority queuing policy.

pqpolicypqTotQueueWaitTime

OID: 1.3.6.1.4.1.5951.4.1.3.7.1.15 Amount of time spent by priority queuing clients waiting in the priority queue.

pqpolicypqTotAvgQueueDepth

OID: 1.3.6.1.4.1.5951.4.1.3.7.1.16 Average number of waiting clients for this priority queuing policy.

pqpolicypqTotAvgQueueWaitTime

OID: 1.3.6.1.4.1.5951.4.1.3.7.1.17 Average wait time for clients for this priority queuing policy.

pqpolicytotClientTransactionTimems

OID: 1.3.6.1.4.1.5951.4.1.3.7.1.18 Total client transaction time in microsec for this priority queuing policy.

pqpolicypqAvgClientTransactionTimems

OID: 1.3.6.1.4.1.5951.4.1.3.7.1.19 Average time taken by a priority queuing client to complete its transaction for this priority queuing policy.

vserverScpolicyTable

OID: 1.3.6.1.4.1.5951.4.1.3.8 The vserver sure connect policy relationship table This is indexed on the svcServiceName and scPolicyName](#)](#)](#) .

vsvrscpolicyPrimaryIPAddress

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.1 The IP address of the service or virtual server to which the policy is bound.

vsvrscpolicyPrimaryPort

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.2 The port of the service or virtual server to which the policy is bound.

vsvrscpolicydesIpAddress

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.8 IP address of the destination service.

vsvrscpolicydestPort

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.9 Port number of the destination service.

vsvrscpolicyavgServerTransactionTime

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.10 Average server transaction time in seconds for this SureConnect Policy.

vsvrscpolicytotClientTransaction

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.11 Total number of client transactions processed by this SureConnect policy.

vsvrscpolicytotOpenConn

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.12 Current number of open connections to the servers matching this policy.

vsvrscpolicyscPhysicalServiceIP

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.13 IP address of the service for which these statistics are maintained.

vsvrscpolicyscPhysicalServicePort

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.14 Port of the service for which these statistics are maintained.

vsvrscpolicyscCurrentWaitingTime

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.15 Value of the currently estimated waiting time in seconds for the configured URL.

vsvrscpolicyscCurrentClientConnections

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.16 Number of clients currently allowed a server connection by this SureConnect policy.

vsvrscpolicyscTotalClientConnections

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.17 Total number of clients that were allowed a server connection by this SureConnect policy.

vsvrscpolicyscTotalServerConnections

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.18 Total number of server connections that were established through this SureConnect policy.

vsvrscpolicyscTotalRequestsReceived

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.19 Total number of requests received by this SureConnect policy.

vsvrscpolicyscTotalRequestBytes

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.20 Total number of request bytes received by this SureConnect policy.

vsvrscpolicyscTotalResponsesReceived

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.21 Total number of server responses received by this SureConnect policy.

vsvrscpolicyscTotalResponseBytes

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.22 Total number of response bytes received by this SureConnect policy.

vsvrscpolicyscCurrentSurgeQClients

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.23 Number of clients currently matching the SureConnect policy, but are in the surge queue.

vsvrscpolicyscCurrentWaitingClients

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.24 Current number of SureConnect priority clients that are waiting for a server connection.

vsvrscpolicyscTotalServerTransactions

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.25 Number of 200 OK responses received from the web server by this SureConnect policy.

vsvrscpolicyscTotalServerTTFBTransactions

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.26 Number of Time-To-First-Byte transcations from the web server for this SureConnect policy.

vsvrscpolicyscTotalServerTTLB

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.27 Server Time-To-Last-Byte in seconds calculated for this SureConnect policy.

vsvrscpolicyscTotalClientTTLB

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.28 Client Time-To-Last-Byte in seconds calculated for this SureConnect policy.

vsvrscpolicyscTotalServerTTFB

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.29 Server Time-To-First-Byte in seconds calculated for this SureConnect policy.

vsvrscpolicyscAverageClientTTLB

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.30 Average value of the client Time-To-Last-Byte in seconds for this SureConnect policy.

vsvrscpolicyscAverageServerTTFB

OID: 1.3.6.1.4.1.5951.4.1.3.8.1.31 Average value of the server Time-To-First-Byte in seconds for this SureConnect policy.

vserverAdvanceSslConfigTable

OID: 1.3.6.1.4.1.5951.4.1.3.9 The vserver advance SSL configuration This is indexed on the vsvrName.

vsvrSslDH

OID: 1.3.6.1.4.1.5951.4.1.3.9.1.1 Whether DH is enabled/disabled.

vsvrSslDHCount

OID: 1.3.6.1.4.1.5951.4.1.3.9.1.2 The DH refresh count to re-generate public/private key.

vsvrSslDHFilePath

OID: 1.3.6.1.4.1.5951.4.1.3.9.1.3 The DH file path name.

vsvrSsleRSA

OID: 1.3.6.1.4.1.5951.4.1.3.9.1.4 The ephimeral RSA support for service.

vsvrSsleRSACount

OID: 1.3.6.1.4.1.5951.4.1.3.9.1.5 The eRSA refresh count to re-generate RSA temporary key.

vsvrSslv2Protocol

OID: 1.3.6.1.4.1.5951.4.1.3.9.1.6 The support for SSLv2 protocol for service.

vsvrSslv3Protocol

OID: 1.3.6.1.4.1.5951.4.1.3.9.1.7 The support for SSLv3 protocol for service.

vsvrSslTLSv1Protocol

OID: 1.3.6.1.4.1.5951.4.1.3.9.1.8 The support for TLSv1 protocol for service.

vsvrSslRedirectSupport

OID: 1.3.6.1.4.1.5951.4.1.3.9.1.9 The support for ssl redirect for service.

vsvrSslClearTextPort

OID: 1.3.6.1.4.1.5951.4.1.3.9.1.10 The clear text port on the backend webserver.

vserverCipherBindingTable

OID: 1.3.6.1.4.1.5951.4.1.3.10 The vserver cipher bindings table This is indexed on the vsvrName and vsvrSslCipherBindName](#)](#) See "Citrix ADC Enterprise OIDs" on page 37 .

vsvrSslCipherBindName

OID: 1.3.6.1.4.1.5951.4.1.3.10.1.1 The cipher name bound to this service.

vsvrSslCipherBindDesc

OID: 1.3.6.1.4.1.5951.4.1.3.10.1.2 The Cipher description.

vserverCsPiPolicyTable

OID: 1.3.6.1.4.1.5951.4.1.3.11 The vserver content switching policy relationship table for PI CS Policy This is indexed on the vsvrName and csPipolicyName](#)](#)](#) .

csPipolicyName

OID: 1.3.6.1.4.1.5951.4.1.3.11.1.1 This represents the name of the CS PI policy bound to content switching vserver

csPipolicyDestVserverName

OID: 1.3.6.1.4.1.5951.4.1.3.11.1.2 This represents the name of the destination vserver to which the request has to be directed to if the content switching policy evaluates to true.

piPolicyBindingHits

OID: 1.3.6.1.4.1.5951.4.1.3.11.1.3 Number of hits on the policy on this binding

csPiIndexVserverFullName

OID: 1.3.6.1.4.1.5951.4.1.3.11.1.4 The full name of the cs vserver to which this policy belongs.

cspolicyActionName

OID: 1.3.6.1.4.1.5951.4.1.3.11.1.5 The name of the CS PI policy action.

snmpTrapVarBindOidsGroup

OID: 1.3.6.1.4.1.5951.4.1.10.2 This is the group of SNMP trap variable bindings.

alarmHighThreshold

OID: 1.3.6.1.4.1.5951.4.1.10.2.1 This is the high threshold value configured for this alarm. When this threshold is crossed an SNMP alarm is generated.

alarmNormalThreshold

OID: 1.3.6.1.4.1.5951.4.1.10.2.2 This is the normal threshold configured for this alarm which triggers the return-to-normal alarm.

entityName

OID: 1.3.6.1.4.1.5951.4.1.10.2.3 This represents the name of the entity whose state has changed.

nsUserName

OID: 1.3.6.1.4.1.5951.4.1.10.2.4 This represents the name of the system user.

configurationCmd

OID: 1.3.6.1.4.1.5951.4.1.10.2.5 This represents the configuartion command that was issued.

authorizationStatus

OID: 1.3.6.1.4.1.5951.4.1.10.2.6 This represents the authorization status for an attempted configuration change.

commandExecutionStatus

OID: 1.3.6.1.4.1.5951.4.1.10.2.7 This represents the command execution status for the attempted configuration change.

unackSynCount

OID: 1.3.6.1.4.1.5951.4.1.10.2.8 The number of un-acknowledged SYNs Citrix ADC has received in the past synFlood time-interval.

alarmLowThreshold

OID: 1.3.6.1.4.1.5951.4.1.10.2.9 This is the low threshold value configured for this alarm. When this threshold is crossed an SNMP alarm is generated.

alarmProbeFailedErrorString

OID: 1.3.6.1.4.1.5951.4.1.10.2.10 This string represents the error occured on the last monitor probe failure.

alarmVipRhiIpAddr

OID: 1.3.6.1.4.1.5951.4.1.10.2.11 This represents the VIP whose RHI state has changed.

alarmVipRhiState

OID: 1.3.6.1.4.1.5951.4.1.10.2.12 This represents the changed RHI state of the VIP.

alarmRateLmtThresholdExceeded

OID: 1.3.6.1.4.1.5951.4.1.10.2.13 This specifies the name of the rate limit identifier that exceeded the threshold.

ipAddressGathered

OID: 1.3.6.1.4.1.5951.4.1.10.2.14 This specifies the list of ip addresses that may have been gathered during the expression evaluation.

stringComputed

OID: 1.3.6.1.4.1.5951.4.1.10.2.15 This contains the string computed during the expression evaluation.

alarmEntityCurState

OID: 1.3.6.1.4.1.5951.4.1.10.2.16 This represents the state of vserver, physicalservice or servicegroup.

sysHealthPowerSupplyStatus

OID: 1.3.6.1.4.1.5951.4.1.10.2.17 This text represents the status of power supply unit

alarmCurrentValue

OID: 1.3.6.1.4.1.5951.4.1.10.2.18 This is the current value of the entity when high or normal threshold trap is sent.

alarmVipRhiInetAddressType

OID: 1.3.6.1.4.1.5951.4.1.10.2.19 The address type of alarmVipRhiInetAddress

alarmVipRhiInetAddress

OID: 1.3.6.1.4.1.5951.4.1.10.2.20 This represents the VIP whose RHI state has changed.

nsClientIPAddr

OID: 1.3.6.1.4.1.5951.4.1.10.2.23 This represents the IP Address of the machine trying to access / connected to Citrix ADC.

ipConflictAddr

OID: 1.3.6.1.4.1.5951.4.1.10.2.24 The IP configured in Citrix ADC conflicting in the network.

appfwLogMsg

OID: 1.3.6.1.4.1.5951.4.1.10.2.25 This represents the log message of appfw check violation.

dnskeyName

OID: 1.3.6.1.4.1.5951.4.1.10.2.26 The name of the DNS key that is due for expiry.

dnskeyTimeToExpire

OID: 1.3.6.1.4.1.5951.4.1.10.2.27 The amount of time for the key to expire

dnskeyUnitsOfExpiry

OID: 1.3.6.1.4.1.5951.4.1.10.2.28 the units of the time of expiry

entityNewName

OID: 1.3.6.1.4.1.5951.4.1.10.2.29 This represents the entity newName after name was changed.

entityOldName

OID: 1.3.6.1.4.1.5951.4.1.10.2.30 This represents the entity Name before name was changed.

platformRateLimitPacketDropCount

OID: 1.3.6.1.4.1.5951.4.1.10.2.31 This counter has the number of packets dropped due to platform rate limiting since the last check.

haLicenseMatchState

OID: 1.3.6.1.4.1.5951.4.1.10.2.32 the state of HA License check

sslCardStatusMsg

OID: 1.3.6.1.4.1.5951.4.1.10.2.33 This represents the interpretation details of sslCardStatus.

callHomeUploadEventStatusMsg

OID: 1.3.6.1.4.1.5951.4.1.10.2.34 This represents the status of CallHome Upload Event.

oldCCOIP

OID: 1.3.6.1.4.1.5951.4.1.10.2.35 This represents the old Configuration Coordinator IP.

newCCOIP

OID: 1.3.6.1.4.1.5951.4.1.10.2.36 This represents the new Configuration Coordinator IP.

oldOVS

OID: 1.3.6.1.4.1.5951.4.1.10.2.37 This represents the old cluster Operational View Set.

newOVS

OID: 1.3.6.1.4.1.5951.4.1.10.2.38 This represents the new Cluster Operational View Set.

qosdVersion

OID: 1.3.6.1.4.1.5951.4.1.10.2.39 This counter tells the QOSD version

brVersion

OID: 1.3.6.1.4.1.5951.4.1.10.2.40 This counter tells the BR version

sslChipName

OID: 1.3.6.1.4.1.5951.4.1.10.2.41 This represents the name of a Crypto device .

vrid

OID: 1.3.6.1.4.1.5951.4.1.10.2.42 This represents the VRID.

vridBoundVIP

OID: 1.3.6.1.4.1.5951.4.1.10.2.43 This represents the VRID bound VIP.

newVridPriority

OID: 1.3.6.1.4.1.5951.4.1.10.2.44 This represents the new priority of VRID

effectiveVridPriority

OID: 1.3.6.1.4.1.5951.4.1.10.2.46 This represents the effective priority of VRID

dstip

OID: 1.3.6.1.4.1.5951.4.1.10.2.47 This is the dstip for which the port allocation has failed.

platformLicensedThroughput

OID: 1.3.6.1.4.1.5951.4.1.10.2.48 This represents the platform licensed throughput.

platformLicensedPPS

OID: 1.3.6.1.4.1.5951.4.1.10.2.49 This represents the platform licensed packets per seconds.

commandFailureReason

OID: 1.3.6.1.4.1.5951.4.1.10.2.50 This is the error string displayed in cli when the command fails.

nsIPAddressType

OID: 1.3.6.1.4.1.5951.4.1.10.2.51 The address type of nsIPAddress

nsIPAddress

OID: 1.3.6.1.4.1.5951.4.1.10.2.52 This represents the IPV6 or IPV4 address.

lsnSubscrIP

OID: 1.3.6.1.4.1.5951.4.1.10.2.53 This represents the LSN Subscriber IP.

lsnSubscrTD

OID: 1.3.6.1.4.1.5951.4.1.10.2.54 This represents the LSN Subscriber TD.

protocol

OID: 1.3.6.1.4.1.5951.4.1.10.2.55 This represents the IP Protocol.

vsvrCurSoValue

OID: 1.3.6.1.4.1.5951.4.1.10.2.56 vserver spillover value.

vsvrSoMethod

OID: 1.3.6.1.4.1.5951.4.1.10.2.57 vserver spillover method.

vsvrSoThresh

OID: 1.3.6.1.4.1.5951.4.1.10.2.58 vserver spillover threshold.

lsnSessLimitExceededBy

OID: 1.3.6.1.4.1.5951.4.1.10.2.59 This represents the entity(group/subscriber) which has exceeded the quota.

nsPartitionName

OID: 1.3.6.1.4.1.5951.4.1.10.2.60 This is the partition name of the source of the trap

operation

OID: 1.3.6.1.4.1.5951.4.1.10.2.61 This represents the operation like add,remove etc

fromPartition

OID: 1.3.6.1.4.1.5951.4.1.10.2.62 This represents the partition name from where switch happened

toPartition

OID: 1.3.6.1.4.1.5951.4.1.10.2.63 This represents the partition name to where switch happened

clPeerID

OID: 1.3.6.1.4.1.5951.4.1.10.2.64 This represents the unique ids of the cluster nodes from where heartbeats are not received on backplane

lsnDSLiteB4Address

OID: 1.3.6.1.4.1.5951.4.1.10.2.65 This represents the IPv6 address of the B4 device in DS-Lite environment.

ipConflictMacAddr

OID: 1.3.6.1.4.1.5951.4.1.10.2.66 The MAC address of the machine having the conflicting IP configured in the network.

gslbSite

OID: 1.3.6.1.4.1.5951.4.1.10.2.67 This represents the GSLB site name.

siteIP

OID: 1.3.6.1.4.1.5951.4.1.10.2.68 This represents the GSLB site IP Address.

lsnNAT64SubscrIPV6

OID: 1.3.6.1.4.1.5951.4.1.10.2.69 This represents the LSN Subscriber IPV6 address.

lsnCurSharedPages

OID: 1.3.6.1.4.1.5951.4.1.10.2.70 This represents the current shared pages in LSN Memory

lsnTotSharedPages

OID: 1.3.6.1.4.1.5951.4.1.10.2.71 This represents the total shared pages in LSN Memory

dnsCacheThreshold

OID: 1.3.6.1.4.1.5951.4.1.10.2.72 This represents the maximum DNS cache threshold that is configured.

dnsCurCacheValue

OID: 1.3.6.1.4.1.5951.4.1.10.2.73 This represents the current DNS cache size used.

sourceIP

OID: 1.3.6.1.4.1.5951.4.1.10.2.74 This represents the source IP of attacker's connection

sourceIPType

OID: 1.3.6.1.4.1.5951.4.1.10.2.75 This represents the type of source IP address.

sourcePort

OID: 1.3.6.1.4.1.5951.4.1.10.2.76 This represents the source port of attacker's connection

gslbSiteName

OID: 1.3.6.1.4.1.5951.4.1.10.2.77 This represents GSLB site name.

gslbSyncStatus

OID: 1.3.6.1.4.1.5951.4.1.10.2.78 This represents GSLB site sync status (success/failure).

urlFilterDbUpdateStatus

OID: 1.3.6.1.4.1.5951.4.1.10.2.79 This represents URLFiltering DB update status (success/failure).

urlfiltDbUpdateErrorCode

OID: 1.3.6.1.4.1.5951.4.1.10.2.80 This represents the Error Code during the URLFiltering DB update.

urlfiltInitSdkStatus

OID: 1.3.6.1.4.1.5951.4.1.10.2.81 This represents the status when initializing the URLFiltering SDK (success/failure).

urlfiltInitSdkErrorCode

OID: 1.3.6.1.4.1.5951.4.1.10.2.82 This represents the Error Code during the URLFiltering SDK initialization.

botLogMsg

OID: 1.3.6.1.4.1.5951.4.1.10.2.83 This represents the log message of Bot check violation.

clusterSyncFailureReason

OID: 1.3.6.1.4.1.5951.4.1.10.2.84 This is the error string displayed when cluster sync failure happens

dstport

OID: 1.3.6.1.4.1.5951.4.1.10.2.85 This represents the destination port

severityLevel

OID: 1.3.6.1.4.1.5951.4.1.10.2.86 This represents the alarm severity level

adcAnomalyId

OID: 1.3.6.1.4.1.5951.4.1.10.2.87 This represents the failure object of the ADC Anomaly.

adcAnomalyMessage

OID: 1.3.6.1.4.1.5951.4.1.10.2.88 This represents the description of the anomaly detected.

dnsZoneName

OID: 1.3.6.1.4.1.5951.4.1.10.2.89 DNS Zone to which key is bound

dnsKeyState

OID: 1.3.6.1.4.1.5951.4.1.10.2.90 DNSSEC Key State

dnskeyStatusMsg

OID: 1.3.6.1.4.1.5951.4.1.10.2.91 Status message

cloudApiFailureErr

OID: 1.3.6.1.4.1.5951.4.1.10.2.92 This is the error string displayed when cloud rest Api failed

Generic MIB-II Traps

‹ Citrix ADC SNMP OID Reference

Generic MIB-II Traps

coldStart (1.3.6.1.6.3.1.1.5.1) A notification is displayed when the Citrix ADC system reinitializes itself.

linkDown (1.3.6.1.6.3.1.1.5.3) A notification is displayed when a network interface on the Citrix ADC system goes down.

linkUp (1.3.6.1.6.3.1.1.5.4) A notification is displayed when a network interface on the Citrix ADC system reinitializes.

authenticationFailure (1.3.6.1.6.3.1.1.5.5) A notification is displayed when a SNMP management application attempts to access the Citrix ADC system and this application does not have access privileges.

Citrix ADC Enterprise Traps

OID:

changeToPrimary

OID:1.3.6.1.4.1.5951.1.1.0.1

This trap indicates that the netscaler is now operating in the primary mode. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm HA-STATE-CHANGE

changeToSecondary

OID:1.3.6.1.4.1.5951.1.1.0.2

This trap indicates that the netscaler is now operating in the Secondary mode. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm HA-STATE-CHANGE

cpuUtilization

OID:1.3.6.1.4.1.5951.1.1.0.3

This trap indicates that the CPU utilization has exceeded the high threshold Varbinds sent in the trap message - nsCPUusage](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#nsCPUusage) , alarmHighThreshold , sysIpAddress To receive this trap enable snmp alarm CPU-USAGE

entitydown

OID:1.3.6.1.4.1.5951.1.1.0.8

This trap is sent when the state of entities such as an interface, vserver, physicalservice or servicegroup changes to DOWN Varbinds sent in the trap message - entityName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#entityName) , sysIpAddress To receive this trap enable snmp alarm ENTITY-STATE

entityup

OID:1.3.6.1.4.1.5951.1.1.0.9

This trap is sent when the state of entities such as an interface, vserver, physicalservice or servicegroup changes to UP Varbinds sent in the trap message - entityName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#entityName) , sysIpAddress To receive this trap enable snmp alarm ENTITY-STATE

synflood

OID:1.3.6.1.4.1.5951.1.1.0.10

This trap is sent when the rate at which unacknowledged SYNs are received cross a threshold value Varbinds sent in the trap message - unackSynCount](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#unackSynCount) , alarmHighThreshold , sysIpAddress To receive this trap enable snmp alarm SYNFLOOD

cpuUtilizationNormal

OID:1.3.6.1.4.1.5951.1.1.0.11

This trap indicates that the CPU utilization has come back to normal Varbinds sent in the trap message - nsCPUusage](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#nsCPUusage) , alarmNormalThreshold , sysIpAddress To receive this trap enable snmp alarm CPU-USAGE

synfloodNormal

OID:1.3.6.1.4.1.5951.1.1.0.12

This trap is sent when the rate at which unacknowledged SYNs are received returns to normal Varbinds sent in the trap message - unackSynCount](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#unackSynCount) , alarmNormalThreshold , sysIpAddress To receive this trap enable snmp alarm SYNFLOOD

memoryUtilization

OID:1.3.6.1.4.1.5951.1.1.0.13

This trap is sent when the memory utilization of the system exceeds the threshold value Varbinds sent in the trap message - resMemUsage](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#resMemUsage) , alarmHighThreshold , sysIpAddress To receive this trap enable snmp alarm MEMORY

memoryUtilizationNormal

OID:1.3.6.1.4.1.5951.1.1.0.14

This trap is sent when the memory utilization of the system returns to normal Varbinds sent in the trap message - resMemUsage](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#resMemUsage) , alarmNormalThreshold , sysIpAddress To receive this trap enable snmp alarm MEMORY

vServerRequestRate

OID:1.3.6.1.4.1.5951.1.1.0.15

This trap is sent when the request rate on a vServer exceeds a threshold value Varbinds sent in the trap message - vsvrName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#vsvrName) , vsvrRequestRate , alarmHighThreshold , vsvrFullName , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm VSERVER-REQRATE

vServerRequestRateNormal

OID:1.3.6.1.4.1.5951.1.1.0.16

This trap is sent when the request rate on a vServer returns to normal Varbinds sent in the trap message - vsvrName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#vsvrName) , vsvrRequestRate , alarmNormalThreshold , vsvrFullName , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm VSERVER-REQRATE

serviceRequestRate

OID:1.3.6.1.4.1.5951.1.1.0.17

This trap is sent when the request rate on a service exceeds a threshold value Varbinds sent in the trap message - svcServiceName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#svcServiceName) , svcRequestRate , alarmHighThreshold , svcServiceFullName , sysIpAddress To receive this trap enable snmp alarm SERVICE-REQRATE

serviceRequestRateNormal

OID:1.3.6.1.4.1.5951.1.1.0.18

This trap is sent when the request rate on a service returns to normal Varbinds sent in the trap message - svcServiceName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#svcServiceName) , svcRequestRate , alarmNormalThreshold , svcServiceFullName , sysIpAddress To receive this trap enable snmp alarm SERVICE-REQRATE

netScalerConfigChange

OID:1.3.6.1.4.1.5951.1.1.0.25

This trap is sent when the configuration on the Citrix ADC is changed. Varbinds sent in the trap message - nsUserName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#nsUserName) , configurationCmd , authorizationStatus , commandExecutionStatus , nsClientIPAddr , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm CONFIG-CHANGE

maxClients

OID:1.3.6.1.4.1.5951.1.1.0.26

This trap is sent when the number of clients hits the maxClients value for a service Varbinds sent in the trap message - svcServiceName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#svcServiceName) , svcEstablishedConn , alarmHighThreshold , svcServiceFullName , sysIpAddress To receive this trap enable snmp alarm SERVICE-MAXCLIENTS

maxClientsNormal

OID:1.3.6.1.4.1.5951.1.1.0.27

This trap is sent when the number of clients falls below 70% of maxClients value for a service. Varbinds sent in the trap message - svcServiceName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#svcServiceName) , svcEstablishedConn , alarmNormalThreshold , svcServiceFullName , sysIpAddress To receive this trap enable snmp alarm SERVICE-MAXCLIENTS

netScalerConfigSave

OID:1.3.6.1.4.1.5951.1.1.0.28

This trap is sent when the configuration on the Citrix ADC is saved. Varbinds sent in the trap message - nsUserName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#nsUserName) , commandExecutionStatus , sysIpAddress To receive this trap enable snmp alarm CONFIG-SAVE

serviceRxBytesRate

OID:1.3.6.1.4.1.5951.1.1.0.29

This trap is sent when the request bytes/s of a service exceeds a threshold value. Varbinds sent in the trap message - svcServiceName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#svcServiceName) , svcRxBytesRate , alarmHighThreshold , svcServiceFullName , sysIpAddress To receive this trap enable snmp alarm ENTITY-RXRATE

serviceRxBytesRateNormal

OID:1.3.6.1.4.1.5951.1.1.0.30

This trap is sent when the request bytes/s of a service returns to normal. Varbinds sent in the trap message - svcServiceName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#svcServiceName) , svcRxBytesRate , alarmNormalThreshold , svcServiceFullName , sysIpAddress To receive this trap enable snmp alarm ENTITY-RXRATE

vserverRxBytesRate

OID:1.3.6.1.4.1.5951.1.1.0.31

This trap is sent when the request bytes/s of a vserver exceeds a threshold value. Varbinds sent in the trap message - vsvrName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#vsvrName) , vsvrRxBytesRate , alarmHighThreshold , vsvrFullName , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm ENTITY-RXRATE

vserverRxBytesRateNormal

OID:1.3.6.1.4.1.5951.1.1.0.32

This trap is sent when the request bytes/s of a vServer returns to normal. Varbinds sent in the trap message - vsvrName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#vsvrName) , vsvrRxBytesRate , alarmNormalThreshold , vsvrFullName , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm ENTITY-RXRATE

serviceTxBytesRate

OID:1.3.6.1.4.1.5951.1.1.0.33

This trap is sent when the response bytes/s of a service exceeds a threshold value. Varbinds sent in the trap message - svcServiceName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#svcServiceName) , svcTxBytesRate , alarmHighThreshold , svcServiceFullName , sysIpAddress To receive this trap enable snmp alarm ENTITY-TXRATE

serviceTxBytesRateNormal

OID:1.3.6.1.4.1.5951.1.1.0.34

This trap is sent when the response bytes/s of a service returns to normal. Varbinds sent in the trap message - svcServiceName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#svcServiceName) , svcTxBytesRate , alarmNormalThreshold , svcServiceFullName , sysIpAddress To receive this trap enable snmp alarm ENTITY-TXRATE

vserverTxBytesRate

OID:1.3.6.1.4.1.5951.1.1.0.35

This trap is sent when the response bytes/s of a vserver exceeds a threshold value. Varbinds sent in the trap message - vsvrName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#vsvrName) , vsvrTxBytesRate , alarmHighThreshold , vsvrFullName , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm ENTITY-TXRATE

vserverTxBytesRateNormal

OID:1.3.6.1.4.1.5951.1.1.0.36

This trap is sent when the response bytes/s of a vServer returns to normal. Varbinds sent in the trap message - vsvrName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#vsvrName) , vsvrTxBytesRate , alarmNormalThreshold , vsvrFullName , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm ENTITY-TXRATE

serviceSynfloodRate

OID:1.3.6.1.4.1.5951.1.1.0.37

This trap is sent when the number of unacknowledged syns for a service exceeds a threshold value. Varbinds sent in the trap message - svcServiceName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#svcServiceName) , svcSynfloodRate , alarmHighThreshold , svcServiceFullName , sysIpAddress To receive this trap enable snmp alarm ENTITY-SYNFLOOD

serviceSynfloodNormal

OID:1.3.6.1.4.1.5951.1.1.0.38

This trap is sent when the number of unacknowledged syns for a service returns to normal. Varbinds sent in the trap message - svcServiceName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#svcServiceName) , svcSynfloodRate , alarmNormalThreshold , svcServiceFullName , sysIpAddress To receive this trap enable snmp alarm ENTITY-SYNFLOOD

vserverSynfloodRate

OID:1.3.6.1.4.1.5951.1.1.0.39

This trap is sent when the number of unacknowledged syns for a vserver exceeds a threshold value. Varbinds sent in the trap message - vsvrName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#vsvrName) , vsvrSynfloodRate , alarmHighThreshold ,

vsvrFullName , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm ENTITY-SYNFLOOD

vserverSynfloodNormal

OID:1.3.6.1.4.1.5951.1.1.0.40

This trap is sent when the number of unacknowledged syns for a vserver returns to normal. Varbinds sent in the trap message - vsvrName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#vsvrName) , vsvrSynfloodRate , alarmNormalThreshold , vsvrFullName , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm ENTITY-SYNFLOOD

svcGroupMemberRequestRate

OID:1.3.6.1.4.1.5951.1.1.0.41

This trap is sent when the request rate on a service group member exceeds a threshold value Varbinds sent in the trap message - svcGrpMemberName , svcGrpMemberRequestRate , alarmHighThreshold , svcGrpMemberFullName , sysIpAddress To receive this trap enable snmp alarm SERVICEGROUP-MEMBER-REQRATE

svcGroupMemberRequestRateNormal

OID:1.3.6.1.4.1.5951.1.1.0.42

This trap is sent when the request rate on a service group member returns to normal Varbinds sent in the trap message - svcGrpMemberName , svcGrpMemberRequestRate , alarmNormalThreshold , svcGrpMemberFullName , sysIpAddress To receive this trap enable snmp alarm SERVICEGROUP-MEMBER-REQRATE

svcGroupMemberRxBytesRate

OID:1.3.6.1.4.1.5951.1.1.0.43

This trap is sent when the request bytes/s of a service group exceeds a threshold value. Varbinds sent in the trap message - svcGrpMemberName , svcGrpMemberRxBytesRate , alarmHighThreshold , svcGrpMemberFullName , sysIpAddress To receive this trap enable snmp alarm ENTITY-RXRATE

svcGroupMemberRxBytesRateNormal

OID:1.3.6.1.4.1.5951.1.1.0.44

This trap is sent when the request bytes/s of a service group returns to normal. Varbinds sent in the trap message - svcGrpMemberName , svcGrpMemberRxBytesRate , alarmNormalThreshold , svcGrpMemberFullName , sysIpAddress To receive this trap enable snmp alarm ENTITY-RXRATE

svcGroupMemberTxBytesRate

OID:1.3.6.1.4.1.5951.1.1.0.45

This trap is sent when the response bytes/s of a service group exceeds a threshold value. Varbinds sent in the trap message - svcGrpMemberName , svcGrpMemberTxBytesRate , alarmHighThreshold , svcGrpMemberFullName , sysIpAddress To receive this trap enable snmp alarm ENTITY-TXRATE

svcGroupMemberTxBytesRateNormal

OID:1.3.6.1.4.1.5951.1.1.0.46

This trap is sent when the response bytes/s of a service group returns to normal. Varbinds sent in the trap message - svcGrpMemberName , svcGrpMemberTxBytesRate , alarmNormalThreshold , svcGrpMemberFullName , sysIpAddress To receive this trap enable snmp alarm ENTITY-TXRATE

svcGroupMemberSynfloodRate

OID:1.3.6.1.4.1.5951.1.1.0.47

This trap is sent when the number of unacknowledged syns for a service group exceeds a threshold value. Varbinds sent in the trap message - svcGrpMemberName , svcGrpMemberSynfloodRate , alarmHighThreshold , svcGrpMemberFullName , sysIpAddress To receive this trap enable snmp alarm ENTITY-SYNFLOOD

svcGroupMemberSynfloodNormal

OID:1.3.6.1.4.1.5951.1.1.0.48

This trap is sent when the number of unacknowledged syns for a service group returns to normal. Varbinds sent in the trap message - svcGrpMemberName , svcGrpMemberSynfloodRate , alarmNormalThreshold , svcGrpMemberFullName , sysIpAddress To receive this trap enable snmp alarm ENTITY-SYNFLOOD

svcGroupMemberMaxClients

OID:1.3.6.1.4.1.5951.1.1.0.49

This trap is sent when the number of clients hits the maxClients value for a service group member Varbinds sent in the trap message - svcGrpMemberName , svcGrpMemberEstablishedConn , alarmHighThreshold , svcGrpMemberFullName , sysIpAddress To receive this trap enable snmp alarm SERVICEGROUP-MEMBER-MAXCLIENTS

svcGroupMemberMaxClientsNormal

OID:1.3.6.1.4.1.5951.1.1.0.50

This trap is sent when the number of clients falls below 70% of maxClients value for a service group member. Varbinds sent in the trap message - svcGrpMemberName , svcGrpMemberEstablishedConn , alarmNormalThreshold , svcGrpMemberFullName , sysIpAddress To receive this trap enable snmp alarm SERVICEGROUP-MEMBER-MAXCLIENTS

averageCpuUtilization

OID:1.3.6.1.4.1.5951.1.1.0.51

This trap indicates that the average CPU usage in the multi-processor Citrix ADC system has exceeded the high threshold. Varbinds sent in the trap message - resCpuUsage](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#resCpuUsage) , alarmHighThreshold , sysIpAddress To receive this trap enable snmp alarm AVERAGE-CPU

averageCpuUtilizationNormal

OID:1.3.6.1.4.1.5951.1.1.0.52

This trap indicates that the average CPU usage in the multi-processor Citrix ADC system has come back to normal. Varbinds sent in the trap message - resCpuUsage](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#resCpuUsage) , alarmNormalThreshold , sysIpAddress To receive this trap enable snmp alarm AVERAGE-CPU

monRespTimeoutAboveThresh

OID:1.3.6.1.4.1.5951.1.1.0.53

This trap is sent when the response timeout for a monitor probe exceeds the configured threshold. Varbinds sent in the trap message - monServiceName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#monServiceName) , monitorName , responseTimeoutThreshold , alarmMonrespto , monitorFullName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#monitorFullName) , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/

citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm MONITOR-RTO-THRESHOLD

monRespTimeoutBelowThresh

OID:1.3.6.1.4.1.5951.1.1.0.54

This trap is sent when the response timeout for a monitor probe comes back to normal, less than the threshold set. Varbinds sent in the trap message - monServiceName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#monServiceName) , monitorName , responseTimeoutThreshold , alarmMonrespto , monitorFullName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#monitorFullName) , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm MONITOR-RTO-THRESHOLD

netScalerLoginFailure

OID:1.3.6.1.4.1.5951.1.1.0.55

This trap is sent when a login attempt to the Citrix ADC fails. Varbinds sent in the trap message - nsUserName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#nsUserName) , nsClientIPAddr , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm LOGIN-FAILURE

sslCertificateExpiry

OID:1.3.6.1.4.1.5951.1.1.0.56

This trap is sent as an advance notification when an SSL certificate is due to expire. Varbinds sent in the trap message - sslCertKeyName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sslCertKeyName) , sslDaysToExpire , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm SSL-CERT-EXPIRY

fanSpeedLow

OID:1.3.6.1.4.1.5951.1.1.0.57

This trap indicates that a fan speed has gone below an alarm threshold. Varbinds sent in the trap message - sysHealthCounterName , sysHealthCounterValue , alarmLowThreshold , sysIpAddress]

(/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm FAN-SPEED-LOW

fanSpeedNormal

OID:1.3.6.1.4.1.5951.1.1.0.58

This trap indicates that a fan speed has returned to normal. Varbinds sent in the trap message - sysHealthCounterName , sysHealthCounterValue , alarmNormalThreshold , sysIpAddress To receive this trap enable snmp alarm FAN-SPEED-LOW

voltageLow

OID:1.3.6.1.4.1.5951.1.1.0.59

This trap indicates that a voltage has gone low. Varbinds sent in the trap message - sysHealthCounterName , sysHealthCounterValue , alarmLowThreshold , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm VOLTAGE-LOW

voltageNormal

OID:1.3.6.1.4.1.5951.1.1.0.60

This trap indicates that a voltage has returned to normal. Varbinds sent in the trap message - sysHealthCounterName , sysHealthCounterValue , alarmNormalThreshold , sysIpAddress To receive this trap enable snmp alarm VOLTAGE-LOW

voltageHigh

OID:1.3.6.1.4.1.5951.1.1.0.61

This trap indicates that a voltage has gone high. Varbinds sent in the trap message - sysHealthCounterName , sysHealthCounterValue , alarmHighThreshold , sysIpAddress To receive this trap enable snmp alarm VOLTAGE-HIGH

temperatureHigh

OID:1.3.6.1.4.1.5951.1.1.0.62

This trap indicates that a temperature has gone high. Varbinds sent in the trap message - sysHealthCounterName , sysHealthCounterValue , alarmHighThreshold , sysIpAddress To receive this trap enable snmp alarm TEMPERATURE-HIGH

temperatureNormal

OID:1.3.6.1.4.1.5951.1.1.0.63

This trap indicates that a temperature has returned to normal. Varbinds sent in the trap message - sysHealthCounterName , sysHealthCounterValue , alarmNormalThreshold , sysIpAddress To receive this trap enable snmp alarm TEMPERATURE-HIGH

diskUsageHigh

OID:1.3.6.1.4.1.5951.1.1.0.64

This trap indicates that disk usage has gone high. Varbinds sent in the trap message - sysHealthDiskName , sysHealthDiskPerusage , alarmHighThreshold , sysIpAddress To receive this trap enable snmp alarm DISK-USAGE-HIGH

diskUsageNormal

OID:1.3.6.1.4.1.5951.1.1.0.65

This trap indicates that disk usage has returned to normal. Varbinds sent in the trap message - sysHealthDiskName , sysHealthDiskPerusage , alarmNormalThreshold , sysIpAddress To receive this trap enable snmp alarm DISK-USAGE-HIGH

interfaceThroughputLow

OID:1.3.6.1.4.1.5951.1.1.0.66

This trap indicates that interface throughput is low. Varbinds sent in the trap message - ifName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#ifName) , ifThroughput , ifMinThroughput](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#ifMinThroughput) , sysIpAddress To receive this trap enable snmp alarm INTERFACE-THROUGHPUT-LOW

interfaceThroughputNormal

OID:1.3.6.1.4.1.5951.1.1.0.67

This trap indicates that interface throughput has returned to normal. Varbinds sent in the trap message - ifName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#ifName) , ifThroughput , ifMinThroughput](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#ifMinThroughput) , sysIpAddress To receive this trap enable snmp alarm INTERFACE-THROUGHPUT-LOW

haVersionMismatch

OID:1.3.6.1.4.1.5951.1.1.0.68

This trap indicates that there is a mismatch in the OS version of the netscalers participating in HA. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm HA-VERSION-MISMATCH

haSyncFailure

OID:1.3.6.1.4.1.5951.1.1.0.69

This trap indicates that config synchronization has failed on secondary. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm HA-SYNC-FAILURE

haNoHeartbeats

OID:1.3.6.1.4.1.5951.1.1.0.70

This trap indicates that HA heartbeats are not received from the secondary. Varbinds sent in the trap message - haNicsMonitorFailed , haLastNicMonitorFailed , sysIpAddress To receive this trap enable snmp alarm HA-NO-HEARTBEATS

haBadSecState

OID:1.3.6.1.4.1.5951.1.1.0.71

This trap indicates that the secondary is in DOWN/UNKNOWN/STAY SECONDARY state. Varbinds sent in the trap message - haPeerSystemState , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm HA-BAD-SECONDARY-STATE

interfaceBWUseHigh

OID:1.3.6.1.4.1.5951.1.1.0.72

This trap is sent when the bandwidth usage of any of the interfaces of the system exceeds the threshold value (configured in Mbits/second) Varbinds sent in the trap message - ifName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#ifName) , alarmHighThreshold , alarmCurrentValue , platformLicensedThroughput , sysIpAddress To receive this trap enable snmp alarm INTERFACE-BW-USAGE

interfaceBWUseNormal

OID:1.3.6.1.4.1.5951.1.1.0.73

This trap is sent when the bandwidth usage of any of the interfaces of the system returns to normal Varbinds sent in the trap message - ifName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#ifName) , alarmNormalThreshold , alarmCurrentValue , platformLicensedThroughput , sysIpAddress To receive this trap enable snmp alarm INTERFACE-BW-USAGE

aggregateBWUseHigh

OID:1.3.6.1.4.1.5951.1.1.0.74

This trap is sent when the aggregate bandwidth usage of the system exceeds the threshold value (configured in Mbits/second) Varbinds sent in the trap message - alarmHighThreshold , alarmCurrentValue , platformLicensedThroughput , sysIpAddress To receive this trap enable snmp alarm INTERFACE-BW-USAGE

aggregateBWUseNormal

OID:1.3.6.1.4.1.5951.1.1.0.75

This trap is sent when the aggregate bandwidth usage of the system returns to normal. Varbinds sent in the trap message - alarmNormalThreshold , alarmCurrentValue , platformLicensedThroughput , sysIpAddress To receive this trap enable snmp alarm INTERFACE-BW-USAGE

vserverRhiStateChange

OID:1.3.6.1.4.1.5951.1.1.0.76

This trap is sent when the vserver RHI state changes. Varbinds sent in the trap message - alarmVipRhiState , alarmVipRhiInetAddressType , alarmVipRhiInetAddress , sysIpAddress To receive this trap enable snmp alarm ENTITY-STATE

rateLmtThresholdExceed

OID:1.3.6.1.4.1.5951.1.1.0.77

This trap is sent when the client exceeds the ratelimit threshold. Varbinds sent in the trap message - alarmRateLmtThresholdExceeded , ipAddressGathered , stringComputed ,

platformLicensedThroughput , sysIpAddress To receive this trap enable snmp alarm RATE-LIMIT-THRESHOLD-EXCEEDED

monProbeFailed

OID:1.3.6.1.4.1.5951.1.1.0.78

This trap is sent when the monitor probe fails for configured number of retries in given max retries attempts. Varbinds sent in the trap message - monServiceName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#monServiceName) , monitorName , alarmProbeFailedRetries , monitorRetrys , alarmProbeFailedErrorString , monitorFullName , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm MON_PROBE_FAILED

temperatureCpuHigh

OID:1.3.6.1.4.1.5951.1.1.0.79

This trap indicates that a CPU temperature has gone high. Varbinds sent in the trap message - sysHealthCounterName , sysHealthCounterValue , alarmHighThreshold , sysIpAddress To receive this trap enable snmp alarm CPU-TEMPERATURE-HIGH

temperatureCpuNormal

OID:1.3.6.1.4.1.5951.1.1.0.80

This trap indicates that a CPU temperature has returned to normal. Varbinds sent in the trap message - sysHealthCounterName , sysHealthCounterValue , alarmNormalThreshold , sysIpAddress To receive this trap enable snmp alarm CPU-TEMPERATURE-HIGH

entityofs

OID:1.3.6.1.4.1.5951.1.1.0.81

This trap is sent when the state of entities such as vserver, physicalservice or servicegroup changes to OUT OF SERVICE Varbinds sent in the trap message - entityName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#entityName) , alarmEntityCurState , sysIpAddress To receive this trap enable snmp alarm ENTITY-STATE

powerSupplyFailed

OID:1.3.6.1.4.1.5951.1.1.0.82

This trap is sent when power supply has failed or disconnected from the system Varbinds sent in the trap message - sysHealthCounterName , sysHealthCounterValue , sysHealthPowerSupplyStatus , sysIpAddress To receive this trap enable snmp alarm POWER-SUPPLY-FAILURE

powerSupplyNormal

OID:1.3.6.1.4.1.5951.1.1.0.83

This trap is sent when power supply status returned back to normal Varbinds sent in the trap message - sysHealthCounterName , sysHealthCounterValue , sysHealthPowerSupplyStatus , sysIpAddress To receive this trap enable snmp alarm POWER-SUPPLY-FAILURE

entityNameChanged

OID:1.3.6.1.4.1.5951.1.1.0.84

This trap is sent when vserver/service/sgroup/lbgroup/server/site entity is renamed Varbinds sent in the trap message - entityName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#entityName) , entityOldName , entityNewName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#entityNewName) , sysIpAddress To receive this trap enable snmp alarm ENTITY-NAME-CHANGE

haPropFailure

OID:1.3.6.1.4.1.5951.1.1.0.85

This trap indicates that config propagation has failed on secondary. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm HA-PROP-FAILURE

ipConflict

OID:1.3.6.1.4.1.5951.1.1.0.86

This trap indicates that ip conflict is present with another device in the network. Varbinds sent in the trap message - ipConflictAddr](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#ipConflictAddr) , ipConflictMacAddr , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm IP-CONFLICT

appfwStartUrl

OID:1.3.6.1.4.1.5951.1.1.0.87

This trap indicates that AppFirewall Start URL violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-START-URL

appfwDenyUrl

OID:1.3.6.1.4.1.5951.1.1.0.88

This trap indicates that AppFirewall Deny URL violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-DENY-URL

appfwRefererHeader

OID:1.3.6.1.4.1.5951.1.1.0.89

This trap indicates that AppFirewall Referer Header violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-REFERER-HEADER

appfwCSRFTag

OID:1.3.6.1.4.1.5951.1.1.0.90

This trap indicates that AppFirewall CSRF Tag violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-CSRF-TAG

appfwCookie

OID:1.3.6.1.4.1.5951.1.1.0.91

This trap indicates that AppFirewall Cookie violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-COOKIE

appfwFieldConsistency

OID:1.3.6.1.4.1.5951.1.1.0.92

This trap indicates that AppFirewall Field Consistency violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-FIELD-CONSISTENCY

appfwBufferOverflow

OID:1.3.6.1.4.1.5951.1.1.0.93

This trap indicates that AppFirewall Buffer Overflow violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-BUFFER-OVERFLOW

appfwFieldFormat

OID:1.3.6.1.4.1.5951.1.1.0.94

This trap indicates that AppFirewall Field Format violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-FIELD-FORMAT

appfwSafeCommerce

OID:1.3.6.1.4.1.5951.1.1.0.95

This trap indicates that AppFirewall Safe Commerce violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-SAFE-COMMERCE

appfwSafeObject

OID:1.3.6.1.4.1.5951.1.1.0.96

This trap indicates that AppFirewall Safe Object violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-SAFE-OBJECT

appfwPolicyHit

OID:1.3.6.1.4.1.5951.1.1.0.97

This trap indicates that AppFirewall Policy Hit occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-POLICY-HIT

appfwXSS

OID:1.3.6.1.4.1.5951.1.1.0.98

This trap indicates that AppFirewall Cross Site Scripting violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-XSS

appfwXMLXSS

OID:1.3.6.1.4.1.5951.1.1.0.99

This trap indicates that AppFirewall XML Cross Site Scripting violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-XML-XSS

appfwSQL

OID:1.3.6.1.4.1.5951.1.1.0.100

This trap indicates that AppFirewall SQL violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-SQL

appfwXMLSQL

OID:1.3.6.1.4.1.5951.1.1.0.101

This trap indicates that AppFirewall XML SQL violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-XML-SQL

appfwXMLAttachment

OID:1.3.6.1.4.1.5951.1.1.0.102

This trap indicates that AppFirewall XML Attachment violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-XML-ATTACHMENT

appfwXMLDos

OID:1.3.6.1.4.1.5951.1.1.0.103

This trap indicates that AppFirewall XML DoS violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-XML-DOS

appfwXMLValidation

OID:1.3.6.1.4.1.5951.1.1.0.104

This trap indicates that AppFirewall XML Validation violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-XML-VALIDATION

appfwXMLWSI

OID:1.3.6.1.4.1.5951.1.1.0.105

This trap indicates that AppFirewall XML WSI violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-XML-WSI

appfwXMLSchemaCompile

OID:1.3.6.1.4.1.5951.1.1.0.106

This trap indicates that AppFirewall XML Schema Compile violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-XML-SCHEMA-COMPILE

appfwXMLSoapFault

OID:1.3.6.1.4.1.5951.1.1.0.107

This trap indicates that AppFirewall XML Soap Fault violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-XML-SOAP-FAULT

dnskeyExpiry

OID:1.3.6.1.4.1.5951.1.1.0.108

This trap is sent as an advance notification when an DNSKEY is due to expire. Varbinds sent in the trap message - dnskeyName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#dnskeyName) , dnskeyTimeToExpire , dnskeyUnitsOfExpiry , sysIpAddress To receive this trap enable snmp alarm DNSKEY-EXPIRY

platformRateLimitThresholdHigh

OID:1.3.6.1.4.1.5951.1.1.0.109

This trap indicates that the platform rate limit (in Mbps) has exceeded the threshold Varbinds sent in the trap message - alarmHighThreshold , alarmCurrentValue , platformLicensedThroughput , sysIpAddress To receive this trap enable snmp alarm PF-RL-RATE-THRESHOLD

platformRateLimitThresholdNormal

OID:1.3.6.1.4.1.5951.1.1.0.110

This trap indicates that the platform rate limit (in Mbps) has come back to normal Varbinds sent in the trap message - alarmNormalThreshold , alarmCurrentValue , platformLicensedThroughput , sysIpAddress To receive this trap enable snmp alarm PF-RL-RATE-THRESHOLD

platformPpsLimitThresholdHigh

OID:1.3.6.1.4.1.5951.1.1.0.111

This trap indicates that the platform packets per second (pps) limit has exceeded the threshold Varbinds sent in the trap message - alarmHighThreshold , alarmCurrentValue , platformLicensedPPS , sysIpAddress To receive this trap enable snmp alarm PF-RL-PPS-THRESHOLD

platformPpsLimitThresholdNormal

OID:1.3.6.1.4.1.5951.1.1.0.112

This trap indicates that the platform packets per second (pps) limit has come back to normal Varbinds sent in the trap message - alarmNormalThreshold , alarmCurrentValue , platformLicensedPPS , sysIpAddress To receive this trap enable snmp alarm PF-RL-PPS-THRESHOLD

platformRateLimitPktDrop

OID:1.3.6.1.4.1.5951.1.1.0.113

This trap is sent when packets are dropped due to platform rate limit (in Mbps) being reached Varbinds sent in the trap message - platformRateLimitPacketDropCount , platformLicensedThroughput , sysIpAddress To receive this trap enable snmp alarm PF-RL-RATE-PKTS-DROPPED

platformPpsLimitPktDrop

OID:1.3.6.1.4.1.5951.1.1.0.114

This trap is sent when packets are dropped due to platform packets per second (pps) limit being reached Varbinds sent in the trap message - platformRateLimitPacketDropCount , platformLicensedPPS , sysIpAddress To receive this trap enable snmp alarm PF-RL-PPS-PKTS-DROPPED

haLicenseCheck

OID:1.3.6.1.4.1.5951.1.1.0.116

This trap is sent when the Citrix ADC comes up and tells the state HA license check whether it is matched or mismatched Varbinds sent in the trap message - haLicenseMatchState , sysIpAddress To receive this trap enable snmp alarm HA-LICENSE-MISMATCH

sslCardFailed

OID:1.3.6.1.4.1.5951.1.1.0.117

This trap is sent when SSL Card has failed Varbinds sent in the trap message - sslCardStatusMsg , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm SSL-CARD-FAILED

sslCardNormal

OID:1.3.6.1.4.1.5951.1.1.0.118

This trap is sent when SSL Card status returned back to normal Varbinds sent in the trap message - sslCardStatusMsg , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm SSL-CARD-NORMAL

warmRestartEvent

OID:1.3.6.1.4.1.5951.1.1.0.119

This trap is sent when a Warm Restart Event occurred Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm WARM-RESTART-EVENT

hardDiskDriveErrors

OID:1.3.6.1.4.1.5951.1.1.0.120

This trap is sent when Hard Disk Drive Errors are seen on the system Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm HARD-DISK-DRIVE-ERRORS

compactFlashErrors

OID:1.3.6.1.4.1.5951.1.1.0.121

This trap is sent when Compact Flash Errors are seen on the system Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm COMPACT-FLASH-ERRORS

callHomeUploadEvent

OID:1.3.6.1.4.1.5951.1.1.0.122

This trap is sent when an attempt to upload Show Tech Support Archive has been made Varbinds sent in the trap message - callHomeUploadEventStatusMsg , sysIpAddress To receive this trap enable snmp alarm CALLHOME-UPLOAD-EVENT

rsa1024KeyExThresholdHigh

OID:1.3.6.1.4.1.5951.1.1.0.123

This trap is sent when RSA 1024 key exchange limit has exceeded the threshold Varbinds sent in the trap message - alarmHighThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm 1024KEY-EXCHANGE-RATE

rsa1024KeyExThresholdNormal

OID:1.3.6.1.4.1.5951.1.1.0.124

This trap is sent when RSA 1024 key exchange limit returns back to normal Varbinds sent in the trap message - alarmNormalThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm 1024KEY-EXCHANGE-RATE

rsa2048KeyExThresholdHigh

OID:1.3.6.1.4.1.5951.1.1.0.125

This trap is sent when RSA 2048 key exchange rate limit has exceeded the threshold Varbinds sent in the trap message - alarmHighThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm 2048KEY-EXCHANGE-RATE

rsa2048KeyExThresholdNormal

OID:1.3.6.1.4.1.5951.1.1.0.126

This trap is sent when RSA 2048 key exchange rate limit returns back to normal Varbinds sent in the trap message - alarmNormalThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm 2048KEY-EXCHANGE-RATE

rsa4096KeyExThresholdHigh

OID:1.3.6.1.4.1.5951.1.1.0.127

This trap is sent when RSA 4096 key exchange rate limit has exceeded the threshold Varbinds sent in the trap message - alarmHighThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm 4096KEY-EXCHANGE-RATE

rsa4096KeyExThresholdNormal

OID:1.3.6.1.4.1.5951.1.1.0.128

This trap is sent when RSA 4096 key exchange rate limit returns back to normal Varbinds sent in the trap message - alarmNormalThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm 4096KEY-EXCHANGE-RATE

sslCurSessionInUseHigh

OID:1.3.6.1.4.1.5951.1.1.0.129

This trap is sent when SSL current session in use has exceeded the threshold Varbinds sent in the trap message - alarmHighThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm SSL-CUR-SESSION-INUSE

sslCurSessionInUseNormal

OID:1.3.6.1.4.1.5951.1.1.0.130

This trap is sent when SSL current session in use returns back to normal Varbinds sent in the trap message - alarmNormalThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm SSL-CUR-SESSION-INUSE

clusterNodeHealth

OID:1.3.6.1.4.1.5951.1.1.0.131

This trap is sent by all cluster nodes when their health state changes. This trap is also sent when a peer node goes down. Varbinds sent in the trap message - clNodeIP](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#clNodeIP) , clNodeEffectiveHealth , clNodeHealthReason , sysIpAddress To receive this trap enable snmp alarm CLUSTER-NODE-HEALTH

clusterNodeQuorum

OID:1.3.6.1.4.1.5951.1.1.0.132

This trap indicates whether the node view of cluster has quorum or not. Varbinds sent in the trap message - clNodeViewQuorum , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/

citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm CLUSTER-NODE-QUORUM

clusterVersionMismatch

OID:1.3.6.1.4.1.5951.1.1.0.133

This trap is sent when there is a version mismatch among the cluster nodes. Varbinds sent in the trap message - clNodeIP](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#clNodeIP) , sysIpAddress To receive this trap enable snmp alarm CLUSTER-VERSION-MISMATCH

clusterCCOChange

OID:1.3.6.1.4.1.5951.1.1.0.134

This trap is sent when the Configuration Coordinator of the cluster changes. Varbinds sent in the trap message - oldCCOIP](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#oldCCOIP) , newCCOIP , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm CLUSTER-CCO-CHANGE

clusterOVSChange

OID:1.3.6.1.4.1.5951.1.1.0.135

This trap is sent when cluster operational view set(OVS) changes. Varbinds sent in the trap message - oldOVS](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#oldOVS) , newOVS , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm CLUSTER-OVS-CHANGE

clusterSyncFailure

OID:1.3.6.1.4.1.5951.1.1.0.136

This trap is sent by cluster nodes when there is a sync failure. Varbinds sent in the trap message - clusterSyncFailureReason , sysIpAddress To receive this trap enable snmp alarm CLUSTER-SYNC-FAILURE

clusterPropFailure

OID:1.3.6.1.4.1.5951.1.1.0.137

This trap is sent when cluster propagation of configurations fails/times out. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm CLUSTER-PROP-FAILURE

stickyPrimary

OID:1.3.6.1.4.1.5951.1.1.0.138

This trap is sent when max flips are completed and we do not give up primary ownership inspite of route monitor failure. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm HA-STICKY-PRIMARY

inbandProtocolVersionMismatch

OID:1.3.6.1.4.1.5951.1.1.0.139

This trap is sent when there is inband protocol mismatch between Qosd and BR. Varbinds sent in the trap message - qosdVersion](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#qosdVersion) , brVersion , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm INBAND-PROTOCOL-VERSION-MISMATCH

sslChipReinit

OID:1.3.6.1.4.1.5951.1.1.0.140

This trap is sent when a SSL chip reinitialize occurs. Varbinds sent in the trap message - sslChipName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sslChipName) , sslChipReinitCount , sysIpAddress To receive this trap enable snmp alarm SSL-CHIP-REINIT

appfwViolations

OID:1.3.6.1.4.1.5951.1.1.0.141

This trap indicates that AppFirewall Unknow Content-Type violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-VIOLATIONS-TYPE

vridStateChange

OID:1.3.6.1.4.1.5951.1.1.0.142

This trap is sent when the state of VRID changes in ACTIVE/ACTIVE setup Varbinds sent in the trap message - vrid](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#vrid) , vridBoundVIP , newVridPriority](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#newVridPriority) , effectiveVridPriority , sysIpAddress To receive this trap enable snmp alarm VRID-STATE-CHANGE

portAllocFailed

OID:1.3.6.1.4.1.5951.1.1.0.143

This trap is sent on port allocation failure Varbinds sent in the trap message - dstip](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#dstip) , sysIpAddress To receive this trap enable snmp alarm PORT-ALLOC-FAILED

lldpRemTablesChange

OID:1.3.6.1.4.1.5951.1.1.0.144

This trap is sent on any insert/delete in lldpRemManAddrTable Varbinds sent in the trap message - nsLLDPRemLocalPortNum , nsLLDPRemChassisId , nsLLDPRemPortId , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm LLDP-REMOTE-CHANGE

ipv6AddressDuplicated

OID:1.3.6.1.4.1.5951.1.1.0.145

This trap indicates that ipv6 address got duplicated in the network. Varbinds sent in the trap message - nsIPAddressType](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#nsIPAddressType) , nsIPAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#nsIPAddress) , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm DUPLICATE-IPV6

lsnPortAllocFailed

OID:1.3.6.1.4.1.5951.1.1.0.146

This trap is sent when a LSN Subscriber is unable to allocate port Varbinds sent in the trap message - lsnGrpName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-

oids#lsnGrpName) , lsnSubscrTD , protocol](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#protocol) , sysIpAddress To receive this trap enable snmp alarm LSN-PORTALLOC-FAILED

lsnPortQuotaExceed

OID:1.3.6.1.4.1.5951.1.1.0.147

This trap is sent when a LSN Subscriber exceeds its Port Quota Varbinds sent in the trap message - lsnGrpName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#lsnGrpName) , lsnSubscrTD , protocol](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#protocol) , sysIpAddress To receive this trap enable snmp alarm LSN-PORTQUOTA-EXCEED

lsnSessionQuotaExceed

OID:1.3.6.1.4.1.5951.1.1.0.148

This trap is sent when a LSN Subscriber exceeds its Session Quota Varbinds sent in the trap message - lsnGrpName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#lsnGrpName) , lsnSubscrTD , protocol](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#protocol) , lsnSessLimitExceededBy , sysIpAddress To receive this trap enable snmp alarm LSN-SESSIONQUOTA-EXCEED

haVersionMatched

OID:1.3.6.1.4.1.5951.1.1.0.149

This trap indicates that the mismatched OS version of the netscalers in HA has been corrected. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm HA-VERSION-MISMATCH

haSyncSucceded

OID:1.3.6.1.4.1.5951.1.1.0.150

This trap indicates that config synchronization has succeded on secondary. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm HA-SYNC-FAILURE

haSecondaryStateNormal

OID:1.3.6.1.4.1.5951.1.1.0.151

This trap indicates that the secondary has come back to normal UP state. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm HA-BAD-SECONDARY-STATE

haHeartbeatsRecvd

OID:1.3.6.1.4.1.5951.1.1.0.152

This trap indicates that Heartbeats have been received on the specified interface. Varbinds sent in the trap message - haNicMonitorSucceeded , sysIpAddress To receive this trap enable snmp alarm HA-NO-HEARTBEATS

vserverSpillOver

OID:1.3.6.1.4.1.5951.1.1.0.153

This trap is sent when the entity(client connections,health,bandwidth etc.) corresponding to the configured spillover method hits the spillover threshold on a vserver Varbinds sent in the trap message - vsvrName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#vsvrName) , vsvrCurSoValue , vsvrSoMethod](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#vsvrSoMethod) , vsvrSoThresh , vsvrFullName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#vsvrFullName) , sysIpAddress To receive this trap enable snmp alarm VSERVER-SPILLOVER

haPropSuccess

OID:1.3.6.1.4.1.5951.1.1.0.154

This trap indicates that config propagation has succeeded on secondary after a previous failure. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm HA-PROP-FAILURE

partitionConfigEvent

OID:1.3.6.1.4.1.5951.1.1.0.155

This trap is sent on partition addition or removal Varbinds sent in the trap message - nsPartitionName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-

oids#nsPartitionName) , operation](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#operation) , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm PARTITION-CONFIG-EVENT

partitionSwitched

OID:1.3.6.1.4.1.5951.1.1.0.156

This trap is sent on partition switching Varbinds sent in the trap message - fromPartition](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#fromPartition) , toPartition , nsUserName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#nsUserName) , sysIpAddress To receive this trap enable snmp alarm PARTITION-SWITCHED

partitionCONNLimitExceeded

OID:1.3.6.1.4.1.5951.1.1.0.157

This trap indicates that the current connection count for the partition has exceeded the configured limit. Varbinds sent in the trap message - alarmHighThreshold , sysIpAddress To receive this trap enable snmp alarm PARTITION-RATE-LIMIT

partitionCONNLimitNormal

OID:1.3.6.1.4.1.5951.1.1.0.158

This trap indicates that the partition can now accept a new connection as per configured limit. Varbinds sent in the trap message - alarmHighThreshold , sysIpAddress To receive this trap enable snmp alarm PARTITION-RATE-LIMIT

partitionBWLimitExceeded

OID:1.3.6.1.4.1.5951.1.1.0.159

This trap is sent when the bandwidth usage of the partition exceeds the configured limit. Varbinds sent in the trap message - alarmHighThreshold , sysIpAddress To receive this trap enable snmp alarm PARTITION-RATE-LIMIT

clusterBackplaneHBMissing

OID:1.3.6.1.4.1.5951.1.1.0.160

This trap is sent when heartbeat is missing on backplane of cluster node Varbinds sent in the trap message - clPeerID](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#clPeerID) , sysIpAddress To receive this trap enable snmp alarm CLUSTER-BACKPLANE-HB-MISSING

pooledLicenseGraceStarted

OID:1.3.6.1.4.1.5951.1.1.0.161

This trap is sent when pooled license is running on grace Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm POOLED-LICENSE-ONGRACE

pooledLicenseGraceNormal

OID:1.3.6.1.4.1.5951.1.1.0.162

This trap is sent when pooled license was running on grace and now it's normal Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm POOLED-LICENSE-ONGRACE

pooledLicenseGracePeriodOver

OID:1.3.6.1.4.1.5951.1.1.0.163

This trap is sent when pooled license was running on grace and it's time period is over Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm POOLED-LICENSE-ONGRACE

pooledLicenseCapacityPartial

OID:1.3.6.1.4.1.5951.1.1.0.164

This trap is sent when system is running on partial capacity Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm POOLED-LICENSE-PARTIAL

pooledLicenseCapacityNormal

OID:1.3.6.1.4.1.5951.1.1.0.165

This trap is sent when system was running on partial capacity and now it has returned to normal Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm POOLED-LICENSE-PARTIAL

gslbSiteMEPflap

OID:1.3.6.1.4.1.5951.1.1.0.166

This trap is sent when the GSLB site MEP flaps. Varbinds sent in the trap message - gslbSite](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#gslbSite) , siteIP , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm GSLB-SITE-MEP-FLAP

lsnMemRecoveryKickedin

OID:1.3.6.1.4.1.5951.1.1.0.167

This trap is sent when a LSN Memory Recovery is kicked in Varbinds sent in the trap message - lsnCurSharedPages , lsnTotSharedPages , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm LSN-MEM-RECOVERY-KICKEDIN

dnsMaxNegCacheLimitHit

OID:1.3.6.1.4.1.5951.1.1.0.168

This trap indicates that the max negative cache allocated for DNS has reached. Varbinds sent in the trap message - dnsCacheThreshold , dnsCurCacheValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm DNS-MAXNEGCACHE-USAGE

dnsMaxCacheLimitHit

OID:1.3.6.1.4.1.5951.1.1.0.169

This trap indicates that the max cache allocated for DNS has reached. Varbinds sent in the trap message - dnsCacheThreshold , dnsCurCacheValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm DNS-MAXCACHE-USAGE

partitionCONNThresholdReached

OID:1.3.6.1.4.1.5951.1.1.0.170

This trap indicates that the number of active connections for this partition has crossed its high threshold limit. Varbinds sent in the trap message - alarmHighThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm PARTITION-RATE-LIMIT

partitionCONNThresholdNormal

OID:1.3.6.1.4.1.5951.1.1.0.171

This trap indicates that the current connection count for the partition is within normal threshold limit. Varbinds sent in the trap message - alarmNormalThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm PARTITION-RATE-LIMIT

partitionBWThresholdReached

OID:1.3.6.1.4.1.5951.1.1.0.172

This trap is sent when the bandwidth usage of the partition exceeds the high threshold limit. Varbinds sent in the trap message - alarmHighThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm PARTITION-RATE-LIMIT

partitionMEMThresholdReached

OID:1.3.6.1.4.1.5951.1.1.0.173

This trap indicates that the memory usage of the partition has crossed its high threshold limit. Varbinds sent in the trap message - nsCPUname](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#nsCPUname) , alarmHighThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm PARTITION-RATE-LIMIT

partitionMEMThresholdNormal

OID:1.3.6.1.4.1.5951.1.1.0.174

This trap indicates that the current memory usage of the partition is within normal threshold limit. Varbinds sent in the trap message - nsCPUname](/en-us/adc-snmp-oid-reference/current-release/

citrix-adc-enterprise-oids#nsCPUname) , alarmNormalThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm PARTITION-RATE-LIMIT

partitionMEMLimitExceeded

OID:1.3.6.1.4.1.5951.1.1.0.175

This trap indicates that the memory usage of the partition has exceeded the configured memory limit. Varbinds sent in the trap message - nsCPUname](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#nsCPUname) , alarmHighThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm PARTITION-RATE-LIMIT

appfwSessionLimit

OID:1.3.6.1.4.1.5951.1.1.0.176

This trap indicates that AppFirewall is operating at Max Session Limit. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-SESSION-LIMIT

tcpSynFloodAttack

OID:1.3.6.1.4.1.5951.1.1.0.177

This trap indicates synflood attack. Varbinds sent in the trap message - unackSynCount](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#unackSynCount) , alarmHighThreshold , sysIpAddress To receive this trap enable snmp alarm TCP-SYNFLOOD

nsLicenseExpiry

OID:1.3.6.1.4.1.5951.1.1.0.178

This trap is sent when Citrix ADC license has expired Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm NS-LICENSE-EXPIRY

pktRateLimitAttack

OID:1.3.6.1.4.1.5951.1.1.0.179

This trap is generated when packet rate limit responder policy detects an attack and drops the connection. Varbinds sent in the trap message - sourceIP](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sourceIP) , sourceIPType , sourcePort](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sourcePort) , sysIpAddress To receive this trap enable snmp alarm PKT-RATELIMITING-ATTACK

gslbSyncStatusFlip

OID:1.3.6.1.4.1.5951.1.1.0.180

This trap is generated when GSLB site sync status changes (success->failure/failure->success). Varbinds sent in the trap message - gslbSiteName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#gslbSiteName) , gslbSyncStatus , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm GSLB-SYNC-STATUS-FLIP

haNoStickyPrimary

OID:1.3.6.1.4.1.5951.1.1.0.181

This trap is sent when ha node comes out of Sticky Primary condition. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm HA-STICKY-PRIMARY

urlfiltDbUpdateStatus

OID:1.3.6.1.4.1.5951.1.1.0.182

This trap is generated when URLFiltering DB is updated. Varbinds sent in the trap message - urlFilterDbUpdateStatus , urlfiltDbUpdateErrorCode , sysIpAddress To receive this trap enable snmp alarm URLFILT-DB-UPDATE-STATUS

urlfiltInitSdk

OID:1.3.6.1.4.1.5951.1.1.0.183

This trap is generated when URLFiltering SDK initializes. Varbinds sent in the trap message - urlfiltInitSdkStatus , urlfiltInitSdkErrorCode , sysIpAddress To receive this trap enable snmp alarm URLFILT-INIT-SDK

clusterSyncSuccess

OID:1.3.6.1.4.1.5951.1.1.0.184

This trap is generate by cluster nodes when there is a change from sync failure to success. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm CLUSTER-SYNC-FAILURE

clusterPropSuccess

OID:1.3.6.1.4.1.5951.1.1.0.185

This trap is sent when cluster propagation state is changed from failure to success. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm CLUSTER-PROP-FAILURE

appfwNewSignatureAdded

OID:1.3.6.1.4.1.5951.1.1.0.186

This trap indicates that new AppFirewall signature has been imported. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-NEW-SIGNATURE-ADDED

pooledLicenseCheckoutFailure

OID:1.3.6.1.4.1.5951.1.1.0.187

This trap is sent when ADC is unable to checkout the configured capacity Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm POOLED-LICENSE-CHECKOUT-FAILURE

pooledLicenseCheckoutSuccess

OID:1.3.6.1.4.1.5951.1.1.0.188

This trap is sent when ADC failed to checkout configured capacity but now it has succeeded and returned to normal Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm POOLED-LICENSE-CHECKOUT-FAILURE

clusterVersionMatched

OID:1.3.6.1.4.1.5951.1.1.0.189

This trap is sent when there is a version mismatch state change Varbinds sent in the trap message - clNodeIP](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#clNodeIP) , sysIpAddress To receive this trap enable snmp alarm CLUSTER-VERSION-MISMATCH

appfwJSONDos

OID:1.3.6.1.4.1.5951.1.1.0.190

This trap indicates that AppFirewall JSON DoS violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-JSON-DOS

appfwJSONSql

OID:1.3.6.1.4.1.5951.1.1.0.191

This trap indicates that AppFirewall JSON SQL violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-JSON-SQL

appfwJSONXss

OID:1.3.6.1.4.1.5951.1.1.0.192

This trap indicates that AppFirewall JSON XSS violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-JSON-XSS

appfwFileUploadTypes

OID:1.3.6.1.4.1.5951.1.1.0.193

This trap indicates that AppFirewall File Upload Types violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-FILE-UPLOAD-TYPE

migrationStarted

OID:1.3.6.1.4.1.5951.1.1.0.194

This trap is sent when Migration is started. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm MIGRATION-STARTED

migrationComplete

OID:1.3.6.1.4.1.5951.1.1.0.195

This trap is sent when Migration is complete on N1. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm MIGRATION-COMPLETE

appfwDeployRelaxationDP

OID:1.3.6.1.4.1.5951.1.1.0.196

This trap indicates that the learned rule is about to be deployed through Dynamic Profiling. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-DEPLOY-RELAXATION-DP

appfwLearnedRuleAppliedDynProf

OID:1.3.6.1.4.1.5951.1.1.0.197

This trap indicates that the learned rule is applied through Dynamic Profiling. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-LEARNED-RULE-APPLIED-DYN-PROF

ecdheTxThresholdHigh

OID:1.3.6.1.4.1.5951.1.1.0.198

This trap is sent when ECDHE based tranactions rate has exceeded the threshold Varbinds sent in the trap message - alarmHighThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm ECDHE-EXCHANGE-RATE

ecdheTxThresholdNormal

OID:1.3.6.1.4.1.5951.1.1.0.199

This trap is sent when ECDHE based tranactions rate returns back to normal Varbinds sent in the trap message - alarmNormalThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm ECDHE-EXCHANGE-RATE

botSignatureUpdate

OID:1.3.6.1.4.1.5951.1.1.0.200

This trap indicates that new Bot signature(s) has been updated. Varbinds sent in the trap message - botLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#botLogMsg) , sysIpAddress To receive this trap enable snmp alarm BOT-SIGNATURE-UPDATE

clusterSyncPartialSuccess

OID:1.3.6.1.4.1.5951.1.1.0.201

This trap is sent by cluster nodes when there is a partial success. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm CLUSTER-SYNC-PARTIAL-SUCCESS

appfwXMLPayloadContentTypeMismatch

OID:1.3.6.1.4.1.5951.1.1.0.202

This trap indicates violations due to Appfw XML Payload Content-Type Mismach. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-XMLPAYLOAD-CONTENT-TYPE-MISMATCH

appfwCMD

OID:1.3.6.1.4.1.5951.1.1.0.203

This trap indicates that AppFirewall CMD violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-CMD

appfwPostBodyLimit

OID:1.3.6.1.4.1.5951.1.1.0.204

This trap indicates that AppFirewall Post Body Limit violation occured. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-POSTBODYLIMIT

appfwSignatureMatch

OID:1.3.6.1.4.1.5951.1.1.0.205

This trap indicates that AppFirewall Signature match violation occured. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-SIGNATURE-MATCH

appfwJSONCmd

OID:1.3.6.1.4.1.5951.1.1.0.206

This trap indicates that AppFirewall JSON Command Injection violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-JSON-CMD

pooledLicenseGraceSevere

OID:1.3.6.1.4.1.5951.1.1.0.207

This trap is sent when pooled license is running on grace for more than 10 days, this duration can be configured by user between 1-30 days Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm POOLED-LICENSE-ONGRACE

appfwSQLGram

OID:1.3.6.1.4.1.5951.1.1.0.208

This trap indicates that AppFirewall SQL Injection violation (reported by SQL Grammar) occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-SQL-GRAM

appfwJSONSQLGram

OID:1.3.6.1.4.1.5951.1.1.0.209

This trap indicates that AppFirewall JSON SQL Injection violation (reported by SQL Grammar) occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-JSON-SQL-GRAM

clusterPropExecFailure

OID:1.3.6.1.4.1.5951.1.1.0.210

This trap indicates that the propagated command has failed on Non-CCO node. Varbinds sent in the trap message - nsUserName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#nsUserName) , configurationCmd , commandExecutionStatus , commandFailureReason , sysIpAddress To receive this trap enable snmp alarm CLUSTER-PROP-EXEC-FAILURE

inconsistentConfigurationInPPEs

OID:1.3.6.1.4.1.5951.1.1.0.211

This trap indicates that configuartion failed in one or more Packet Processing Engine and created configuration inconsistency among Packet Processing Engines. Varbinds sent in the trap message - configurationCmd , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm INCONSISTENT-CONFIGURATION-IN-PPES

portAllocExceed

OID:1.3.6.1.4.1.5951.1.1.0.212

This trap is sent if port allocation exceeds the configured threshold value Varbinds sent in the trap message - dstip](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#dstip) , dstport , protocol](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#protocol) , sysIpAddress To receive this trap enable snmp alarm PORT-ALLOC-EXCEED

appfwGRPC

OID:1.3.6.1.4.1.5951.1.1.0.213

This trap indicates that AppFirewall caught an invalid gRPC request. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-GRPC

appfwCMDGram

OID:1.3.6.1.4.1.5951.1.1.0.214

This trap indicates that AppFirewall CMD Injection violation (reported by CMD Grammar) occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-CMD-GRAM

appfwJSONCMDGram

OID:1.3.6.1.4.1.5951.1.1.0.215

This trap indicates that AppFirewall JSON CMD Injection violation (reported by CMD Grammar) occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-JSON-CMD-GRAM

appfwBlockKeyword

OID:1.3.6.1.4.1.5951.1.1.0.216

This trap indicates that AppFirewall Block Keyword violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-BLOCK-KEYWORD

updateKEKSuccess

OID:1.3.6.1.4.1.5951.1.1.0.217

This trap indicates that Update KEK operation was successful. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm KEK_UPDATE_SUCCESS

updateKEKFailure

OID:1.3.6.1.4.1.5951.1.1.0.218

This trap indicates that Update KEK operation failed. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm KEK_UPDATE_FAILURE

appfwJSONBlockKeyword

OID:1.3.6.1.4.1.5951.1.1.0.219

This trap indicates that AppFirewall JSON Block Keyword violation occurred. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-JSON-BLOCKKEYWORD

appfwGRPCText

OID:1.3.6.1.4.1.5951.1.1.0.220

This trap indicates that AppFirewall caught an invalid gRPC Web Text request. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-GRPC-WEB-TEXT

appfwGRPCJSON

OID:1.3.6.1.4.1.5951.1.1.0.221

This trap indicates that AppFirewall caught an invalid gRPC Web JSON request. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-GRPC-WEB-JSON

adcAnomaly

OID:1.3.6.1.4.1.5951.1.1.0.222

This trap is sent when an ADC Anomaly is detected. Varbinds sent in the trap message - adcAnomalyId](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#adcAnomalyId) , adcAnomalyMessage , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm ADC-ANOMALY

adcAnomalyClear

OID:1.3.6.1.4.1.5951.1.1.0.223

This trap is sent when an ADC Anomaly is cleared off. Varbinds sent in the trap message - adcAnomalyId](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#adcAnomalyId) , adcAnomalyMessage , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm ADC-ANOMALY

syslogConnectionDropped

OID:1.3.6.1.4.1.5951.1.1.0.224

This trap indicates that connection between syslog and server has dropped. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm SYSLOG-CONNECTION-DROPPED

appfwBypassList

OID:1.3.6.1.4.1.5951.1.1.0.225

This trap indicates that AppFirewall Bypass List Rule has hit. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-BYPASS-LIST

appfwDenyList

OID:1.3.6.1.4.1.5951.1.1.0.226

This trap indicates that AppFirewall Deny List Rule has hit. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-DENY-LIST

nsrootPasswordExpiryWarning

OID:1.3.6.1.4.1.5951.1.1.0.227

This trap indicates that nsroot password is expired or about to expire. Varbinds sent in the trap message - sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm NSROOT_PASSWORD_EXPIRY_WARNING

dnskeyStChgFailed

OID:1.3.6.1.4.1.5951.1.1.0.228

This trap is sent whenever there is a failed change in DNSSEC KEY State. Varbinds sent in the trap message - dnskeyName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#dnskeyName) , dnsZoneName , dnsKeyState](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#dnsKeyState) , dnskeyStatusMsg , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm DNSSEC-KEY-AUTOMGMT-STATUS-FAILURE

dnskeyStChgSuccess

OID:1.3.6.1.4.1.5951.1.1.0.229

This trap is sent whenever there is a successful change in DNSSEC KEY State. Varbinds sent in the trap message - dnskeyName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#dnskeyName) , dnsZoneName , dnsKeyState](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#dnsKeyState) , dnskeyStatusMsg , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm DNSSEC-KEY-AUTOMGMT-STATUS-SUCCESS

cloudApiFailure

OID:1.3.6.1.4.1.5951.1.1.0.230

This trap indicates that Cloud Rest Api Triggered from PE is failed which result in inconsistency in Cloud setup. Varbinds sent in the trap message - cloudApiFailureErr , sysIpAddress To receive this trap enable snmp alarm CLOUD-REST-API-FAILURE

appfwSchemaEndpointNotFound

OID:1.3.6.1.4.1.5951.1.1.0.231

This trap indicates that AppFirewall Schema validation failed. Endpoint not found in the API spec. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-SCHEMA-ENDPOINT-NOTFOUND

appfwSchemaMethodUnSupported

OID:1.3.6.1.4.1.5951.1.1.0.232

This trap indicates that AppFirewall Schema validation failed. Method is not supported as per the API spec. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-SCHEMA-METHOD-UNSUPPORTED

appfwSchemaParameterMissing

OID:1.3.6.1.4.1.5951.1.1.0.233

This trap indicates that AppFirewall Schema validation failed. Required parameter(s) is missing as per the API Spec. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-SCHEMA-PARAMETER-MISSING

appfwSchemaValueInCorrect

OID:1.3.6.1.4.1.5951.1.1.0.234

This trap indicates that AppFirewall Schema validation failed. Parameter Value is incorrect as per the API Spec. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-SCHEMA-VALUE-INCORRECT

appfwSchemaContentTypeUnSupported

OID:1.3.6.1.4.1.5951.1.1.0.235

This trap indicates that AppFirewall Schema validation failed. Content-type is unsupported as per the API Spec. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-SCHEMA-CONTENTTYPE-UNSUPPORTED

appfwSchemaParameterInvalid

OID:1.3.6.1.4.1.5951.1.1.0.236

This trap indicates that AppFirewall Schema validation failed. Parameter is invalid as per the API spec. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-SCHEMA-PARAMETER-INVALID

appfwSchemaOther

OID:1.3.6.1.4.1.5951.1.1.0.237

This trap indicates that AppFirewall Schema validation failed. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-SCHEMA-OTHER

appfwSchemaRelaxationRule

OID:1.3.6.1.4.1.5951.1.1.0.238

This trap indicates that AppFirewall Schema Relaxation Rule Hit. Varbinds sent in the trap message - appfwLogMsg](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#appfwLogMsg) , sysIpAddress To receive this trap enable snmp alarm APPFW-SCHEMA-RELAXATION-RULE

asymCryptoUtilHigh

OID:1.3.6.1.4.1.5951.1.1.0.239

This trap is sent when asymmetric crypto utilization has exceeded the threshold Varbinds sent in the trap message - alarmHighThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm SSL-ASYM-CRYPTO-UTILIZATION

asymCryptoUtilNormal

OID:1.3.6.1.4.1.5951.1.1.0.240

This trap is sent when asymmetric crypto utilization has returned to normal Varbinds sent in the trap message - alarmHighThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm SSL-ASYM-CRYPTO-UTILIZATION

symCryptoUtilHigh

OID:1.3.6.1.4.1.5951.1.1.0.241

This trap is sent when symmetric crypto utilization has exceeded the threshold Varbinds sent in the trap message - alarmHighThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-

reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm SSL-SYM-CRYPTO-UTILIZATION

symCryptoUtilNormal

OID:1.3.6.1.4.1.5951.1.1.0.242

This trap is sent when symmetric crypto utilization has returned to normal Varbinds sent in the trap message - alarmHighThreshold , alarmCurrentValue , sysIpAddress](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#sysIpAddress) To receive this trap enable snmp alarm SSL-SYM-CRYPTO-UTILIZATION

interfaceAutoRecovered

OID:1.3.6.1.4.1.5951.1.1.0.243

This trap indicates the VF interface got AutoRecovered from an Error-Disabled state Varbinds sent in the trap message - ifName](/en-us/adc-snmp-oid-reference/current-release/citrix-adc-enterprise-oids#ifName) , sysIpAddress To receive this trap enable snmp alarm INTERFACE-AUTO-RECOVERY