NetScaler SNMP OID Reference

Jan 10, 2017

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

    - nsPbr6Table
  - gslbGlobalStats
  - nsPolicyStatsTable
  - nsDnsServerStatsGroup
  - nsdnsRegisterTable
  - scPolicyStatistics
  - sslCertKeyTable
  - sslCrlTable
  - sslCipherGroupTable
  - dosPolicyTable
  - dosPolicyStatistics
  - pqPolicyConfigTable
  - pqPolicyStatistics
  - crPolicyMapConfigTable
  - appFirewallStatistics
  - appfwProfileTable
  - nsRnatGlobalStats
  - nsRnatPerIPStatsTable
  - piPolicyTable
  - nsInatGlobalStats
  - nsInatPerNat46StatsTable
  - nsInatPerNatStatsTable
  - nsNat64GlobalStats
  - nsLLDPConfigGroup
  - nsLLDPStatsGroup
    - nsLLDPStatsTxPortTable
    - nsLLDPStatsRxPortTable
  - nsLLDPLocSystemsGroup
    - nsLLDPLocPortTable
    - nsLLDPLocManAddrTable
  - nsLsnGlobalStatsGroup
  - nsLsnGroupTable
  - nsPPTPStatsGroup
  - nsLsnDSLiteGlobalStatsGroup
  - nsLsnLogStatsGroup
    - nsLsnMappingLogStatsGroup
    - nsLsnSessionLogStatsGroup
  - gslbSitesTable
  - nsDomainTable
  - scPolicyConfigTable
  - nsLLDPRemTable
  - nsLLDPRemManAddrTable
- serviceTable
- serverTable
- serviceScpolicyTable
- serviceAdvanceSslConfigTable
- serviceCipherBindingTable
- serviceGlobalStatsGroup
- serviceGroupMemberTable
- serviceDospolicyTable
- monitorMemberTable
- monServiceMemberTable
- serviceGroupTable
- vserverTable
- vserverServiceTable
- vserverCspolicyTable
- vserverCrpolicyTable
- vserverGlobalStatsGroup
- lbvserverTable
- vserverPqpolicyTable
- vserverScpolicyTable

Note: Refer to the Hardware documentation for the recommended range for the hardware attributes.

Generic MIB-II OIDs

system (1.3.6.1.2.1.1)

sysDescr (1.3.6.1.2.1.1.1)

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

sysObjectID (1.3.6.1.2.1.1.2)

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

sysUpTime (1.3.6.1.2.1.1.3)

The time (in hundredths of a second) since the network management portion of the system was last re-initialized.

sysContact (1.3.6.1.2.1.1.4)

The textual identification of the contact person for

this managed node, together with information on how to contact this person. If no contact information is known, the value is the zero-length string.

sysName (1.3.6.1.2.1.1.5)

An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string.

sysLocation (1.3.6.1.2.1.1.6)

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

sysServices (1.3.6.1.2.1.1.7)

A value which indicates the set of services that this entity may potentially offer. The value is a sum. This sum initially takes the value zero. Then, for each layer, L, in the range 1 through 7, that this node performs transactions for, 2 raised to (L - 1) is added to the sum. For example, a node which performs only routing functions would have a value of 4 (2^(3-1)). In contrast, a node which is a host offering application services would have a value of 72 (2^(4-1) + 2^(7-1)). Note that in the context of the Internet suite of protocols, values should be calculated accordingly:

layer functionality

1 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 6

may also be counted.

snmp (1.3.6.1.2.1.11)

snmpInPkts (1.3.6.1.2.1.11.1)

The total number of messages delivered to the SNMP

entity from the transport service.

snmpInBadVersions (1.3.6.1.2.1.11.3)

The total number of SNMP messages which were delivered

to the SNMP entity and were for an unsupported SNMP

version.

snmpInBadCommunityNames (1.3.6.1.2.1.11.4)

The total number of community-based SNMP messages (for

example, SNMPv1) delivered to the SNMP entity which

used an SNMP community name not known to said entity.

Also, implementations which authenticate community-based

SNMP messages using check(s) in addition to matching

the community name (for example, by also checking

whether the message originated from a transport address

allowed to use a specified community name) MAY include

in this value the number of messages which failed the

additional check(s). It is strongly RECOMMENDED that

the documentation for any security model which is used

to authenticate community-based SNMP messages specify

the precise conditions that contribute to this value.

snmpInBadCommunityUses (1.3.6.1.2.1.11.5)

The total number of community-based SNMP messages (for

example, SNMPv1) delivered to the SNMP entity which represented an SNMP operation that was not allowed for the SNMP community named in the message. The precise conditions under which this counter is incremented (if at all) depend on how the SNMP entity implements its access control mechanism and how its applications interact with that access control mechanism. It is strongly RECOMMENDED that the documentation for any access control mechanism which is used to control access to and visibility of MIB instrumentation specify the precise conditions that contribute to this value.

snmpInASNParseErrs (1.3.6.1.2.1.11.6)

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

snmpEnableAuthenTraps (1.3.6.1.2.1.11.30)

Indicates whether the SNMP entity is permitted to generate authenticationFailure traps. The value of this object overrides any configuration information; as such, it provides a means whereby all authenticationFailure traps may be disabled.

Note that it is strongly recommended that this object be stored in non-volatile memory so that it remains constant across re-initializations of the network management system.

snmpSilentDrops (1.3.6.1.2.1.11.31)

The total number of Confirmed Class PDUs (such as GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and

InformRequest-PDUs) delivered to the SNMP entity which were silently dropped because the size of a reply containing an alternate Response Class PDU (such as a Response-PDU) with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.

snmpProxyDrops (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, and InformRequest-PDUs) delivered to the SNMP entity which were silently dropped because the transmission of the (possibly translated) message to a proxy target failed in a manner (other than a time-out) such that no Response Class PDU (such as a Response-PDU) could be returned.

interfaces (1.3.6.1.2.1.2)

ifNumber (1.3.6.1.2.1.2.1)

The number of network interfaces (regardless of their current state) present on this system.

ifTable (1.3.6.1.2.1.2.2)

A list of interface entries. The number of entries is given by the value of ifNumber.

ifIndex (1.3.6.1.2.1.2.2.1.1)

A unique value, greater than zero, for each interface. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer

must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization.

ifDescr (1.3.6.1.2.1.2.2.1.2)

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

ifType (1.3.6.1.2.1.2.2.1.3)

The type of interface. Additional values for ifType are assigned by the Internet Assigned Numbers Authority (IANA), through updating the syntax of the IANAifType textual convention.

ifMtu (1.3.6.1.2.1.2.2.1.4)

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

ifSpeed (1.3.6.1.2.1.2.2.1.5)

An estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth. If the bandwidth of the interface is greater than the maximum value reportable by this object then this object should report its maximum value (4,294,967,295) and ifHighSpeed must be used to report the interace's speed. For a sub-layer which has

no concept of bandwidth, this object should be zero.

ifPhysAddress (1.3.6.1.2.1.2.2.1.6)

The interface's address at its protocol sub-layer. For example, for an 802.x interface, this object normally contains a MAC address. The interface's media-specific MIB must define the bit and byte ordering and the format of the value of this object. For interfaces which do not have such an address (e.g., a serial line), this object should contain an octet string of zero length.

ifAdminStatus (1.3.6.1.2.1.2.2.1.7)

The desired state of the interface. The testing(3) state indicates that no operational packets can be passed. When a managed system initializes, all interfaces start with ifAdminStatus in the down(2) state. As a result of either explicit management action or per configuration information retained by the managed system, ifAdminStatus is then changed to either the up(1) or testing(3) states (or remains in the down(2) state).

ifOperStatus (1.3.6.1.2.1.2.2.1.8)

The current operational state of the interface. The testing(3) state indicates that no operational packets can be passed. If ifAdminStatus is down(2) then ifOperStatus should be down(2). If ifAdminStatus is changed to up(1) then ifOperStatus should change to up(1) if the interface is ready to transmit and receive network traffic; it should change to dormant(5) if the interface is waiting for external actions (such as a serial line waiting for an incoming connection); it should remain in the down(2) state

if and only if there is a fault that prevents it from going to the up(1) state; it should remain in the notPresent(6) state if the interface has missing (typically, hardware) components.

ifLastChange (1.3.6.1.2.1.2.2.1.9)

The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this object contains a zero value.

ifInOctets (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 at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime.

ifInUcastPkts (1.3.6.1.2.1.2.2.1.11)

The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer.
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.

ifInDiscards (1.3.6.1.2.1.2.2.1.13)

The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent

their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

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.

ifInErrors (1.3.6.1.2.1.2.2.1.14)

For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.

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.

ifInUnknownProtos (1.3.6.1.2.1.2.2.1.15)

For packet-oriented interfaces, the number of packets received via the interface which were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing the number of transmission units received via the interface which were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter will always be 0.

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.

ifOutOctets (1.3.6.1.2.1.2.2.1.16)

The total number of octets transmitted out of the interface, including framing characters.

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.

ifOutUcastPkts (1.3.6.1.2.1.2.2.1.17)

The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.

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.

ifOutDiscards (1.3.6.1.2.1.2.2.1.19)

The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.

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.

ifOutErrors (1.3.6.1.2.1.2.2.1.20)

For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

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.

ifMIBObjects (1.3.6.1.2.1.31.1)

ifTableLastChange (1.3.6.1.2.1.31.1.5)

The value of sysUpTime at the time of the last creation or deletion of an entry in the ifTable. If the number of entries has been unchanged since the last re-initialization of the local network management subsystem, then this object contains a zero value.

ifXTable (1.3.6.1.2.1.31.1.1)

A list of interface entries. The number of entries is given by the value of ifNumber. This table contains additional objects for the interface table.

ifInMulticastPkts (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 (1.3.6.1.2.1.31.1.1.1.3)

The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.

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.

ifOutMulticastPkts (1.3.6.1.2.1.31.1.1.1.4)

The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. 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.

ifOutBroadcastPkts (1.3.6.1.2.1.31.1.1.1.5)

The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.

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.

ifHCInOctets (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-bit version of ifInOctets.

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.

ifHCInUcastPkts (1.3.6.1.2.1.31.1.1.1.7)

The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were not addressed to a multicast or broadcast address at this sub-layer. This object is a 64-bit version of ifInUcastPkts.

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.

ifHCInMulticastPkts (1.3.6.1.2.1.31.1.1.1.8)

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. This object is a 64-bit version of ifInMulticastPkts.

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.

ifHCInBroadcastPkts (1.3.6.1.2.1.31.1.1.1.9)

The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer. This object is a 64-bit version of ifInBroadcastPkts.

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.

ifHCOutOctets (1.3.6.1.2.1.31.1.1.1.10)

The total number of octets transmitted out of the interface, including framing characters. This object is a 64-bit version of ifOutOctets.

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.

ifHCOutUcastPkts (1.3.6.1.2.1.31.1.1.1.11)

The total number of packets that higher-level protocols requested be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of ifOutUcastPkts.

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.

ifHCOutMulticastPkts (1.3.6.1.2.1.31.1.1.1.12)

The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent. For a MAC layer protocol, this includes both Group and Functional addresses. This object is a 64-bit version of ifOutMulticastPkts.

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.

ifHCOutBroadcastPkts (1.3.6.1.2.1.31.1.1.1.13)

The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent. This object is a 64-bit version of ifOutBroadcastPkts.

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.

ifLinkUpDownTrapEnable (1.3.6.1.2.1.31.1.1.1.14)

Indicates whether linkUp/linkDown traps should be generated for this interface.

By default, this object should have the value enabled(1) for interfaces which do not operate on 'top' of any other interface (as defined in the ifStackTable), and disabled(2) otherwise.

ifHighSpeed (1.3.6.1.2.1.31.1.1.1.15)

An estimate of the interface's current bandwidth in units
of 1,000,000 bits per second. If this object reports a
value of `n' then the speed of the interface is somewhere in
the range of `n-500,000' to `n+499,999'. For interfaces
which do not vary in bandwidth or for those where no
accurate estimation can be made, this object should contain
the nominal bandwidth. For a sub-layer which has no concept
of bandwidth, this object should be zero.

ifPromiscuousMode (1.3.6.1.2.1.31.1.1.1.16)

This object has a value of false(2) if this interface only
accepts packets/frames that are addressed to this station.
This object has a value of true(1) when the station accepts
all packets/frames transmitted on the media. The value
true(1) is only legal on certain types of media. If legal,
setting this object to a value of true(1) may require the
interface to be reset before becoming effective.
The value of ifPromiscuousMode does not affect the reception
of broadcast and multicast packets/frames by the interface.

ifConnectorPresent (1.3.6.1.2.1.31.1.1.1.17)

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

ifAlias (1.3.6.1.2.1.31.1.1.1.18)

This object is an 'alias' name for the interface as
specified by a network manager, and provides a non-volatile
'handle' for the interface.
On the first instantiation of an interface, the value of

ifAlias associated with that interface is the zero-length string. As and when a value is written into an instance of ifAlias through a network management set operation, then the agent must retain the supplied value in the ifAlias instance associated with the same interface for as long as that interface remains instantiated, including across all re-initializations/reboots of the network management system, including those which result in a change of the interface's ifIndex value.

An example of the value which a network manager might store in this object for a WAN interface is the (Telco's) circuit number/identifier of the interface.

Some agents may support write-access only for interfaces having particular values of ifType. An agent which supports write access to this object is required to keep the value in non-volatile storage, but it may limit the length of new values depending on how much storage is already occupied by the current values for other interfaces.

ifCounterDiscontinuityTime (1.3.6.1.2.1.31.1.1.1.19)

The value of sysUpTime on the most recent occasion at which any one or more of this interface's counters suffered a discontinuity. The relevant counters are the specific instances associated with this interface of any Counter32 or Counter64 object contained in the ifTable or ifXTable. If no such discontinuities have occurred since the last re-initialization of the local management subsystem, then this object contains a zero value.

icmp (1.3.6.1.2.1.5)

udp (1.3.6.1.2.1.7)

udpInDatagrams (1.3.6.1.2.1.7.1)

The total number of UDP datagrams delivered to UDP users.

Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by discontinuities in the value of sysUpTime.

udpNoPorts (1.3.6.1.2.1.7.2)

The total number of received UDP datagrams for which there was no application at the destination port.

Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by discontinuities in the value of sysUpTime.

udpInErrors (1.3.6.1.2.1.7.3)

The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.

Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by discontinuities in the value of sysUpTime.

udpOutDatagrams (1.3.6.1.2.1.7.4)

The total number of UDP datagrams sent from this entity.

Discontinuities in the value of this counter can occur at re-initialization of the management system, and at

other times as indicated by discontinuities in the value of sysUpTime.

Generic MIB-II Traps

coldStart (1.3.6.1.6.3.1.1.5.1)

A coldStart trap signifies that the SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.

linkDown (1.3.6.1.6.3.1.1.5.3)

A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus.

Varbinds sent in the trap message: ifIndex, ifAdminStatus, ifOperStatus

linkUp (1.3.6.1.6.3.1.1.5.4)

A linkUp trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links left the down state and transitioned into some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus.

Varbinds sent in the trap message: ifIndex, ifAdminStatus, ifOperStatus

authenticationFailure (1.3.6.1.6.3.1.1.5.5)

An authenticationFailure trap signifies that the SNMP entity has received a protocol message that is not properly authenticated. While all implementations

of SNMP entities MAY be capable of generating this

trap, the snmpEnableAuthenTraps object indicates

whether this trap will be generated.

NetScaler Enterprise Traps

changeToPrimary (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

To receive this trap, enable the following SNMP alarm: HA-STATE-CHANGE

changeToSecondary (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

To receive this trap, enable the following SNMP alarm: HA-STATE-CHANGE

cpuUtilization (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, alarmHighThreshold, sysIpAddress

To receive this trap, enable the following SNMP alarm: CPU-USAGE

entitydown (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: ENTITY-STATE

entityup (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: ENTITY-STATE

synflood (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, alarmHighThreshold, sysIpAddress

To receive this trap, enable the following SNMP alarm: SYNFLOOD

cpuUtilizationNormal (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, alarmNormalThreshold, sysIpAddress

To receive this trap, enable the following SNMP alarm: CPU-USAGE

synfloodNormal (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, alarmNormalThreshold, sysIpAddress

To receive this trap, enable the following SNMP alarm: SYNFLOOD

memoryUtilization (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, alarmHighThreshold, sysIpAddress

To receive this trap, enable the following SNMP alarm: MEMORY

memoryUtilizationNormal (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, alarmNormalThreshold, sysIpAddress

To receive this trap, enable the following SNMP alarm: MEMORY

vServerRequestRate (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, vsvrRequestRate, alarmHighThreshold, vsvrFullName, sysIpAddress

To receive this trap, enable the following SNMP alarm: VSERVER-REQRATE

vServerRequestRateNormal (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, vsvrRequestRate, alarmNormalThreshold, vsvrFullName, sysIpAddress

To receive this trap, enable the following SNMP alarm: VSERVER-REQRATE

serviceRequestRate (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, svcRequestRate, alarmHighThreshold, svcServiceFullName, sysIpAddress

To receive this trap, enable the following SNMP alarm: SERVICE-REQRATE

serviceRequestRateNormal (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, svcRequestRate, alarmNormalThreshold, svcServiceFullName, sysIpAddress

To receive this trap, enable the following SNMP alarm: SERVICE-REQRATE

netScalerConfigChange (1.3.6.1.4.1.5951.1.1.0.25)

This trap is sent when the configuration on the NetScaler is changed.

Varbinds sent in the trap message: nsUserName, configurationCmd, authorizationStatus, commandExecutionStatus, nsClientIPAddr, sysIpAddress

To receive this trap, enable the following SNMP alarm: CONFIG-CHANGE

maxClients (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, svcEstablishedConn, alarmHighThreshold, svcServiceFullName, sysIpAddress

To receive this trap, enable the following SNMP alarm: SERVICE-MAXCLIENTS

maxClientsNormal (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, svcEstablishedConn, alarmNormalThreshold, svcServiceFullName, sysIpAddress

To receive this trap, enable the following SNMP alarm: SERVICE-MAXCLIENTS

netScalerConfigSave (1.3.6.1.4.1.5951.1.1.0.28)

This trap is sent when the configuration on the NetScaler is saved.

Varbinds sent in the trap message: nsUserName, sysIpAddress

To receive this trap, enable the following SNMP alarm: CONFIG-SAVE

serviceRxBytesRate (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, svcRxBytesRate, alarmHighThreshold, svcServiceFullName, sysIpAddress

To receive this trap, enable the following SNMP alarm: ENTITY-RXRATE

serviceRxBytesRateNormal (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, svcRxBytesRate, alarmNormalThreshold, svcServiceFullName, sysIpAddress

To receive this trap, enable the following SNMP alarm: ENTITY-RXRATE

vserverRxBytesRate (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, vsvrRxBytesRate, alarmHighThreshold, vsvrFullName, sysIpAddress

To receive this trap, enable the following SNMP alarm: ENTITY-RXRATE

vserverRxBytesRateNormal (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, vsvrRxBytesRate, alarmNormalThreshold, vsvrFullName, sysIpAddress

To receive this trap, enable the following SNMP alarm: ENTITY-RXRATE

serviceTxBytesRate (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, svcTxBytesRate, alarmHighThreshold, svcServiceFullName, sysIpAddress

To receive this trap, enable the following SNMP alarm: ENTITY-TXRATE

serviceTxBytesRateNormal (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, svcTxBytesRate, alarmNormalThreshold, svcServiceFullName, sysIpAddress

To receive this trap, enable the following SNMP alarm: ENTITY-TXRATE

vserverTxBytesRate (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, vsvrTxBytesRate, alarmHighThreshold, vsvrFullName, sysIpAddress

To receive this trap, enable the following SNMP alarm: ENTITY-TXRATE

vserverTxBytesRateNormal (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, vsvrTxBytesRate, alarmNormalThreshold, vsvrFullName, sysIpAddress

To receive this trap, enable the following SNMP alarm: ENTITY-TXRATE

serviceSynfloodRate (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, svcSynfloodRate, alarmHighThreshold, svcServiceFullName, sysIpAddress

To receive this trap, enable the following SNMP alarm: ENTITY-SYNFLOOD

serviceSynfloodNormal (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, svcSynfloodRate, alarmNormalThreshold, svcServiceFullName, sysIpAddress

To receive this trap, enable the following SNMP alarm: ENTITY-SYNFLOOD

vserverSynfloodRate (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, vsvrSynfloodRate, alarmHighThreshold, vsvrFullName, sysIpAddress

To receive this trap, enable the following SNMP alarm: ENTITY-SYNFLOOD

vserverSynfloodNormal (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, vsvrSynfloodRate, alarmNormalThreshold, vsvrFullName, sysIpAddress

To receive this trap, enable the following SNMP alarm: ENTITY-SYNFLOOD

svcGroupMemberRequestRate (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 the following SNMP alarm: SERVICEGROUP-MEMBER-REQRATE

svcGroupMemberRequestRateNormal (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 the following SNMP alarm: SERVICEGROUP-MEMBER-REQRATE

svcGroupMemberRxBytesRate (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 the following SNMP alarm: ENTITY-RXRATE

svcGroupMemberRxBytesRateNormal (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 the following SNMP alarm: ENTITY-RXRATE

svcGroupMemberTxBytesRate (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 the following SNMP alarm: ENTITY-TXRATE

svcGroupMemberTxBytesRateNormal (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 the following SNMP alarm: ENTITY-TXRATE

svcGroupMemberSynfloodRate (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 the following SNMP alarm: ENTITY-SYNFLOOD

svcGroupMemberSynfloodNormal (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 the following SNMP alarm: ENTITY-SYNFLOOD

svcGroupMemberMaxClients (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 the following SNMP alarm: SERVICEGROUP-MEMBER-MAXCLIENTS

svcGroupMemberMaxClientsNormal (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 the following SNMP alarm: SERVICEGROUP-MEMBER-MAXCLIENTS

averageCpuUtilization (1.3.6.1.4.1.5951.1.1.0.51)

This trap indicates that the average CPU usage in the multi-processor NetScaler system has exceeded the high threshold.

Varbinds sent in the trap message: resCpuUsage, alarmHighThreshold, sysIpAddress

To receive this trap, enable the following SNMP alarm: AVERAGE-CPU

averageCpuUtilizationNormal (1.3.6.1.4.1.5951.1.1.0.52)

This trap indicates that the average CPU usage in the multi-processor NetScaler system has come back to normal.

Varbinds sent in the trap message: resCpuUsage, alarmNormalThreshold, sysIpAddress

To receive this trap, enable the following SNMP alarm: AVERAGE-CPU

monRespTimeoutAboveThresh (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, monitorName, responseTimeoutThreshold, alarmMonrespto, sysIpAddress

To receive this trap, enable the following SNMP alarm: MONITOR-RTO-THRESHOLD

monRespTimeoutBelowThresh (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, monitorName, responseTimeoutThreshold, alarmMonrespto, sysIpAddress

To receive this trap, enable the following SNMP alarm: MONITOR-RTO-THRESHOLD

netScalerLoginFailure (1.3.6.1.4.1.5951.1.1.0.55)

This trap is sent when a login attempt to the NetScaler fails.

Varbinds sent in the trap message: nsUserName, sysIpAddress

To receive this trap, enable the following SNMP alarm: LOGIN-FAILURE

sslCertificateExpiry (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, sslDaysToExpire, sysIpAddress

To receive this trap, enable the following SNMP alarm: SSL-CERT-EXPIRY

fanSpeedLow (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

To receive this trap, enable the following SNMP alarm: FAN-SPEED-LOW

fanSpeedNormal (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 the following SNMP alarm: FAN-SPEED-LOW

voltageLow (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

To receive this trap, enable the following SNMP alarm: VOLTAGE-LOW

voltageNormal (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 the following SNMP alarm: VOLTAGE-LOW

voltageHigh (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 the following SNMP alarm: VOLTAGE-HIGH

temperatureHigh (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 the following SNMP alarm: TEMPERATURE-HIGH

temperatureNormal (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 the following SNMP alarm: TEMPERATURE-HIGH

diskUsageHigh (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 the following SNMP alarm: DISK-USAGE-HIGH

diskUsageNormal (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 the following SNMP alarm: DISK-USAGE-HIGH

interfaceThroughputLow (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, ifThroughput, ifMinThroughput, sysIpAddress

To receive this trap, enable the following SNMP alarm: INTERFACE-THROUGHPUT-LOW

interfaceThroughputNormal (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, ifThroughput, ifMinThroughput, sysIpAddress

To receive this trap, enable the following SNMP alarm: INTERFACE-THROUGHPUT-LOW

haVersionMismatch (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

To receive this trap, enable the following SNMP alarm: HA-VERSION-MISMATCH

haSyncFailure (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

To receive this trap, enable the following SNMP alarm: HA-SYNC-FAILURE

haNoHeartbeats (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 the following SNMP alarm: HA-NO-HEARTBEATS

haBadSecState (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

To receive this trap, enable the following SNMP alarm: HA-BAD-SECONDARY-STATE

interfaceBWUseHigh (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, alarmHighThreshold, alarmCurrentValue, platformLicensedThroughput, sysIpAddress

To receive this trap, enable the following SNMP alarm: INTERFACE-BW-USAGE

interfaceBWUseNormal (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, alarmNormalThreshold, alarmCurrentValue, platformLicensedThroughput, sysIpAddress

To receive this trap, enable the following SNMP alarm: INTERFACE-BW-USAGE

aggregateBWUseHigh (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 the following SNMP alarm: INTERFACE-BW-USAGE

aggregateBWUseNormal (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 the following SNMP alarm: INTERFACE-BW-USAGE

vserverRhiStateChange (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 the following SNMP alarm: ENTITY-STATE

rateLmtThresholdExceed (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 the following SNMP alarm: RATE-LIMIT-THRESHOLD-EXCEEDED

monProbeFailed (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, monitorName, alarmProbeFailedRetries, monitorRetrys, alarmProbeFailedErrorString, sysIpAddress

To receive this trap, enable the following SNMP alarm: MON_PROBE_FAILED

temperatureCpuHigh (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 the following SNMP alarm: CPU-TEMPERATURE-HIGH

temperatureCpuNormal (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 the following SNMP alarm: CPU-TEMPERATURE-HIGH

entityofs (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, alarmEntityCurState, sysIpAddress

To receive this trap, enable the following SNMP alarm: ENTITY-STATE

powerSupplyFailed (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 the following SNMP alarm: POWER-SUPPLY-FAILURE

powerSupplyNormal (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 the following SNMP alarm: POWER-SUPPLY-FAILURE

entityNameChanged (1.3.6.1.4.1.5951.1.1.0.84)

This trap is sent when vserver/service/sgroup/lbgroup/server entity is renamed

Varbinds sent in the trap message: entityName, entityOldName, entityNewName, sysIpAddress

To receive this trap, enable the following SNMP alarm: ENTITY-NAME-CHANGE

haPropFailure (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

To receive this trap, enable the following SNMP alarm: HA-PROP-FAILURE

ipConflict (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: IP-CONFLICT

appfwStartUrl (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-START-URL

appfwDenyUrl (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-DENY-URL

appfwRefererHeader (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-REFERER-HEADER

appfwCSRFTag (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-CSRF-TAG

appfwCookie (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-COOKIE

appfwFieldConsistency (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-FIELD-CONSISTENCY

appfwBufferOverflow (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-BUFFER-OVERFLOW

appfwFieldFormat (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-FIELD-FORMAT

appfwSafeCommerce (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-SAFE-COMMERCE

appfwSafeObject (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-SAFE-OBJECT

appfwPolicyHit (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-POLICY-HIT

appfwXSS (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-XSS

appfwXMLXSS (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-XML-XSS

appfwSQL (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-SQL

appfwXMLSQL (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-XML-SQL

appfwXMLAttachment (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-XML-ATTACHMENT

appfwXMLDos (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-XML-DOS

appfwXMLValidation (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-XML-VALIDATION

appfwXMLWSI (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-XML-WSI

appfwXMLSchemaCompile (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-XML-SCHEMA-COMPILE

appfwXMLSoapFault (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-XML-SOAP-FAULT

dnskeyExpiry (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, dnskeyTimeToExpire, dnskeyUnitsOfExpiry, sysIpAddress

To receive this trap, enable the following SNMP alarm: DNSKEY-EXPIRY

platformRateLimitThresholdHigh (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 the following SNMP alarm: PF-RL-RATE-THRESHOLD

platformRateLimitThresholdNormal (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 the following SNMP alarm: PF-RL-RATE-THRESHOLD

platformPpsLimitThresholdHigh (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 the following SNMP alarm: PF-RL-PPS-THRESHOLD

platformPpsLimitThresholdNormal (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 the following SNMP alarm: PF-RL-PPS-THRESHOLD

platformRateLimitPktDrop (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 the following SNMP alarm: PF-RL-RATE-PKTS-DROPPED

platformPpsLimitPktDrop (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 the following SNMP alarm: PF-RL-PPS-PKTS-DROPPED

DataStreamRateLimitHit (1.3.6.1.4.1.5951.1.1.0.115)

DateStream Rate-Limiting is Removed. So, this trap is not required.

haLicenseCheck (1.3.6.1.4.1.5951.1.1.0.116)

This trap is sent when the NetScaler 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 the following SNMP alarm: HA-LICENSE-MISMATCH

sslCardFailed (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

To receive this trap, enable the following SNMP alarm: SSL-CARD-FAILED

sslCardNormal (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

To receive this trap, enable the following SNMP alarm: SSL-CARD-NORMAL

warmRestartEvent (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

To receive this trap, enable the following SNMP alarm: WARM-RESTART-EVENT

hardDiskDriveErrors (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

To receive this trap, enable the following SNMP alarm: HARD-DISK-DRIVE-ERRORS

compactFlashErrors (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

To receive this trap, enable the following SNMP alarm: COMPACT-FLASH-ERRORS

callHomeUploadEvent (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 the following SNMP alarm: CALLHOME-UPLOAD-EVENT

rsa1024KeyExThresholdHigh (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

To receive this trap, enable the following SNMP alarm: 1024KEY-EXCHANGE-RATE

rsa1024KeyExThresholdNormal (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

To receive this trap, enable the following SNMP alarm: 1024KEY-EXCHANGE-RATE

rsa2048KeyExThresholdHigh (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

To receive this trap, enable the following SNMP alarm: 2048KEY-EXCHANGE-RATE

rsa2048KeyExThresholdNormal (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

To receive this trap, enable the following SNMP alarm: 2048KEY-EXCHANGE-RATE

rsa4096KeyExThresholdHigh (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

To receive this trap, enable the following SNMP alarm: 4096KEY-EXCHANGE-RATE

rsa4096KeyExThresholdNormal (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

To receive this trap, enable the following SNMP alarm: 4096KEY-EXCHANGE-RATE

sslCurSessionInUseHigh (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

To receive this trap, enable the following SNMP alarm: SSL-CUR-SESSION-INUSE

sslCurSessionInUseNormal (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

To receive this trap, enable the following SNMP alarm: SSL-CUR-SESSION-INUSE

clusterNodeHealth (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, clNodeEffectiveHealth, clNodeHealthReason, sysIpAddress

To receive this trap, enable the following SNMP alarm: CLUSTER-NODE-HEALTH

clusterNodeQuorum (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

To receive this trap, enable the following SNMP alarm: CLUSTER-NODE-QUORUM

clusterVersionMismatch (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: CLUSTER-VERSION-MISMATCH

clusterCCOChange (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, newCCOIP, sysIpAddress

To receive this trap, enable the following SNMP alarm: CLUSTER-CCO-CHANGE

clusterOVSChange (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, newOVS, sysIpAddress

To receive this trap, enable the following SNMP alarm: CLUSTER-OVS-CHANGE

clusterSyncFailure (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: sysIpAddress

To receive this trap, enable the following SNMP alarm: CLUSTER-SYNC-FAILURE

clusterPropFailure (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

To receive this trap, enable the following SNMP alarm: CLUSTER-PROP-FAILURE

stickyPrimary (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

To receive this trap, enable the following SNMP alarm: HA-STICKY-PRIMARY

inbandProtocolVersionMismatch (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, brVersion, sysIpAddress

To receive this trap, enable the following SNMP alarm: INBAND-PROTOCOL-VERSION-MISMATCH

sslChipReinit (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, sslChipReinitCount, sysIpAddress

To receive this trap, enable the following SNMP alarm: SSL-CHIP-REINIT

appfwViolations (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: APPFW-VIOLATIONS-TYPE

vridStateChange (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, vridBoundVIP, newVridPriority, effectiveVridPriority, sysIpAddress

To receive this trap, enable the following SNMP alarm: VRID-STATE-CHANGE

portAllocFailed (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: PORT-ALLOC-FAILED

lldpRemTablesChange (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: lldpRemLocalPortNum, lldpRemChassisId, lldpRemPortId, sysIpAddress

To receive this trap, enable the following SNMP alarm: LLDP-REMOTE-CHANGE

ipv6AddressDuplicated (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, nsIPAddress, sysIpAddress

To receive this trap, enable the following SNMP alarm: DUPLICATE-IPV6

lsnPortAllocFailed (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, lsnSubscrIP, lsnSubscrTD, protocol, sysIpAddress

To receive this trap, enable the following SNMP alarm: LSN-PORTALLOC-FAILED

lsnPortQuotaExceed (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, lsnSubscrIP, lsnSubscrTD, protocol, sysIpAddress

To receive this trap, enable the following SNMP alarm: LSN-PORTQUOTA-EXCEED

lsnSessionQuotaExceed (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, lsnSubscrIP, lsnSubscrTD, protocol, lsnSessLimitExceededBy, sysIpAddress

To receive this trap, enable the following SNMP alarm: LSN-SESSIONQUOTA-EXCEED

haVersionMatched (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

To receive this trap, enable the following SNMP alarm: HA-VERSION-MISMATCH

haSyncSucceded (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

To receive this trap, enable the following SNMP alarm: HA-SYNC-FAILURE

haSecondaryStateNormal (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

To receive this trap, enable the following SNMP alarm: HA-BAD-SECONDARY-STATE

haHeartbeatsRecvd (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 the following SNMP alarm: HA-NO-HEARTBEATS

vserverSpillOver (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, vsvrCurSoValue, vsvrSoMethod, vsvrSoThresh, vsvrFullName, sysIpAddress

To receive this trap, enable the following SNMP alarm: VSERVER-SPILLOVER

haPropSuccess (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

To receive this trap, enable the following SNMP alarm: HA-PROP-FAILURE

partitionConfigEvent (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, operation, sysIpAddress

To receive this trap, enable the following SNMP alarm: PARTITION-CONFIG-EVENT

partitionSwitched (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, toPartition, nsUserName, sysIpAddress

To receive this trap, enable the following SNMP alarm: PARTITION-SWITCHED

partitionCONNLimitExceeded (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 the following SNMP alarm: PARTITION-RATE-LIMIT

partitionCONNLimitNormal (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 the following SNMP alarm: PARTITION-RATE-LIMIT

partitionBWLimitExceeded (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 the following SNMP alarm: PARTITION-RATE-LIMIT

clusterBackplaneHBMissing (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, sysIpAddress

To receive this trap, enable the following SNMP alarm: CLUSTER-BACKPLANE-HB-MISSING

Handling Long Table Index Names

As per RFC 2578, all OIDs are limited to 128 sub-identifiers. This places some limitations on table indexing because this also applies to OIDs for object instances, and these consist of the concatenation of the base OID assigned in the object definition plus the index components. Therefore in case of tables, if the length of the index name on which an SNMP request is made is greater than 31 characters, it is encoded using an internal encoding function. As a result, the encoded name will be displayed in the SNMP Manager. However, the table will provide an additional FullName OID by querying which it is possible to get back the original index name on which the query was made. For example – While performing SNMP GET operation on vserverTable using the index vserverName, if the vserverName is greater than 31 characters, it is encoded. However, vserverTable provides an OID - vsvrFullName (1.3.6.1.4.1.5951.4.1.3.1.1.59), by querying which it is possible to get back the original vserver name. The following tables are indexed on index names which follow the above behaviour.

- nsPolicyStatsTable
- vserverTable
- lbvserverTable
- serviceAdvanceSslConfigTable
- serverTable
- serviceTable
- serviceGroupTable
- piPolicyTable
- vserverCspolicyTable
- vserverCspolicyTable
- vserverCrpolicyTable
- vserverScpolicyTable
- serviceGroupMemberTable
- vserverCipherBindingTable
- serviceCipherBindingTable